MOUNT PLEASANT COTTAGE SCHOOL UNION FREE SCHOOL DISTRICT

SUBJECT: STUDENT DATA BREACHES: PREVENTION, RESPONSE AND NOTIFICATION

School Districts have a legal responsibility to protect the privacy of education data, including Personally Identifiable Information (PII) of its students, in both paper and electronic formats. Although the Family Education Rights and Privacy Act (FERPA) does not include specific data breach notification requirements, it does protect the confidentiality of education records by requiring districts to record each incident of data disclosure in accordance with 34 CFR 99.32 (a)(1). A breach of student data maintained electronically would be considered such a "disclosure" that must be recorded. In addition, under state law, direct notification to parents and/or affected students may be warranted depending on the type of data compromised, such as student social security numbers and/or other identifying information that could lead to identity theft.

The following guidelines will assist the School District in efforts to prevent student data breaches and guide the response and notification protocol should a student data breach occur.

Definitions

"Data Breach" is any instance in which there is an unauthorized release of or access to Personally Identifiable Information (PII) from student education records or other protected information about students not suitable for public release.

"Education Records" are records directly related to a student and maintained by an education agency or institution, or by a party acting on behalf of the agency or institution.

"Personally Identifiable Information (PII)" from education records includes information, such as a student's name or identification number, that can be used to distinguish or trace an individual's identity either directly or indirectly through linkages with other information. PII includes an individual's name, identification number, social security number, date and place of birth, mothers' maiden name, biometric records, etc.

Also refer to Regulation #7240R -- Access to Student Records for additional definitions and information related to student records and FERPA.

Prevention of Student Data Breaches

Incident Response Team

The District may choose to assemble an incident response team within the District to deal with possible data breaches. The team may designate a manager who will be in charge of incident response and at least one (1) other person who can assume authority in the absence of the manager. Staff will be notified of the team and the method of contact in the event of a breach. The team will also be available

(Continued)

SUBJECT: STUDENT DATA BREACHES: PREVENTION, RESPONSE AND NOTIFICATION (Cont'd.)

to staff to answer questions and develop strategies to prevent and detect a breach. The team will establish roles and responsibilities, specify access credentials, work with the Superintendent to coordinate the flow of information, and manage the District's public message in the event of a breach.

Review Information Systems and Data

The District, in conjunction with appropriate staff (such as the Chief Information Officer, the Records Officer, and/or technology coordinator) will review information systems and data to identify where Personally Identifiable Information (PII) is stored and used. The review may involve:

1) Documenting what PII and other sensitive information is maintained by the District, where it is stored (including backup and archived data), and how it is kept secure;

2) Conducting regular risk assessments and evaluating privacy threats for the District;

3) Reviewing those approved for access to PII and/or other sensitive information and checking user activity status to determine which accounts should be deactivated after a pre-determined period of inactivity;

4) Reviewing separation of duties to help ensure integrity of security checks and balances;

5) Implementing mitigation controls designed to prevent and detect unauthorized access, theft, or misuse of PII and/or other sensitive data;

6) Implementing security controls, such as encryption of sensitive data in motion and at rest (where feasible); and

7) Regularly reviewing and updating data destruction policies to minimize the risk of data breaches through unauthorized access to archived records or computers that are no longer in use.

Monitor Sensitive Data Leakage and Loss

The District will also monitor for PII and other sensitive data leakage and loss. This may include:

1) Employing automated tools, such as intrusion detection and prevention systems, next generation firewalls, and anti-virus and anti-malware tools, to monitor and alert about suspicious or anomalous activity;

(Continued)

SUBJECT: STUDENT DATA BREACHES: PREVENTION, RESPONSE AND NOTIFICATION (Cont'd.)

2) Using data loss prevention solutions to track the movement and use of information within the District's system, to detect and prevent the unintentional disclosure of PII and/or other sensitive data, for both data at rest and data in motion;

3) Conducting regular searches of the information system and physical storage areas to identify PII that may be outside of approved areas (i.e., scan networks for policy violations or occasionally police open areas for PII left unattended on desks);

4) Conducting internet searches to locate (and, whenever possible, remove) information that is already in the public domain or visible to the public; and

5) Periodically testing and checking privacy and information security controls (i.e., through the use of "real-life" exercises) to validate their effectiveness as part of a risk management program.

Conduct Privacy and Security Awareness Training

The District may conduct privacy and security awareness training. This may include:

1) Providing privacy and information security training on a recurring basis to appropriate staff involved in data-related activities;

2) Posting and communicating privacy policies to parents, students, staff and other users (i.e., on the District Web page, on a bulletin board at the office, or through statements inserted in documents or emails, etc.); and

3) Clearly defining and making easily accessible processes for reporting privacy incidents and complaints.

Response to Student Data Breaches

In the event that information from student education records may have been compromised or inadvertently disclosed, the District may take one or more of the following steps suggested by the U.S. Department of Education, as deemed necessary under the particular circumstances. The following list is not meant to be linear or all inclusive:

1) Validate or confirm the data breach and determine exactly what information was compromised (i.e., names, addresses, social security numbers, ID numbers, credit card numbers, grades, and the like).

(Continued)

SUBJECT: STUDENT DATA BREACHES: PREVENTION, RESPONSE AND NOTIFICATION (Cont'd.)

2) Assemble an incident response team to coordinate all aspects of the breach response.

3) Take steps immediately to determine affected devices, retrieve data, and prevent any further disclosures.

4) Identify all affected records and students. Locate, obtain, and preserve for examination all written and electronic logs and records applicable to the breach.

5) Determine how the incident occurred, including which school officials had control of and responsibility for the information that was compromised. Determine whether the incident occurred because of a lack of monitoring and oversight.

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

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

8) Consult with the District's School Attorney to ensure compliance with any applicable federal, state and/or local laws or regulations related to data breaches, reporting or notification requirements.

9) Report the incident to law enforcement authorities if criminal activity is suspected. If law enforcement is involved, coordinate investigations and evidence collection to avoid compromising outcomes.

Notification of Student Data Breaches

In the event of a student data breach, the District will determine whether notification is warranted or required and when it should be made, pursuant to federal, state, and local laws. If the compromised data includes student social security numbers in combination with other identifying information that could lead to identity theft, the District may directly notify affected students and/or their parents of the breach and notify students and their parents that the U.S. Education Department's Office of Inspector General maintains a website describing steps students may take if they suspect they are a victim of identity theft at: http://www.ed.gov/about/offices/list/oig/misused/idtheft.html and http://www.ed.gov/about/offices/list/oig/misused/victim.html.

The District shall maintain a record of each incident of data disclosure in accordance with 34 CFR 99.32 (a)(1).

(Continued)

SUBJECT: STUDENT DATA BREACHES: PREVENTION, RESPONSE AND NOTIFICATION (Cont'd.)

Consider Notification of FPCO and PTAC

The incident response team may consider notifying the Family Policy Compliance Office (FPCO) about the breach. The FPCO can assist School Districts by helping to determine the potential for harm from the release of the information. The incident response team may also consider seeking technical assistance from the Privacy Technical Assistance Center (PTAC) for support with security and breach prevention. Additional information from PTAC is available at www.ed.gov/ptac.

If the breach involves student data protected under state law, or data other than student educational records, refer to Regulation #5672R -- Data Breach Investigation and Notification Process.

NOTE: A portion of the above guidelines have been adapted from the "Data Breach Response Checklist" from the U.S. Education Department's Privacy Technical Assistance Center. This information should be used as a general guide, and is meant to be customized to the School District's unique operational security needs in consultation with appropriate legal counsel.