FREDERICK COUNTY PUBLIC SCHOOLS	Reg. No. 200-31
Subject: **DATA BREACH RESPONSE PROCESS**	**Issued:** **2/22/17**
Preparing Office: **Office of the Superintendent**	**Amended:**

Policy 207

I. For purposes of this regulation, breach of security of a system is defined as "the unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of the personal information maintained by Frederick County Public Schools (FCPS)."

II. Procedures

The Superintendent will initiate a prompt investigation of any allegation of breach of security of an FCPS system and provide notice to affected individuals and federal/state agencies as stipulated in law.

A. Validation of the Breach

Upon notification of an alleged breach, a prompt investigation by the Director of Technology Infrastructure will commence to determine if a breach occurred.

B. Response to a Breach

If a breach has been validated, the Director of Technology Infrastructure will act as the incident manager and coordinate the proper notification to law enforcement, state and federal agencies, and insurance carriers. The incident response team working with the Director of Technology Infrastructure shall include:

- Supervisor of Security and Emergency Management
- Chief of Staff and Legal Counsel
- Deputy Superintendent
- Superintendent
- Director of Communications, Community Engagement and Marketing
- Chief Financial Officer
- Designated Data Owner [1]

C. Mitigation Efforts

Once the status of the breach is determined (i.e. ongoing, active or post breach), the Director of Technology Infrastructure will take all necessary steps to ensure further data loss is mitigated by securing and blocking unauthorized access to

[1] Data owner refers to an individual within an organization in direct control of that data and is responsible for authorizing access to or dissemination, integrity and accuracy of the data (i.e., Director of System Accountability and School Improvement - student data, Chief Financial Officer – financial data, Executive Director of Human Resources - employee data).

systems data and preservation of evidence for investigation and protocol is followed as established under paragraph E below.

All steps will be thoroughly documented to ensure full compliance and cooperation with law enforcement investigations and preserve evidence for potential insurance related claims.

D. Confidentiality

All FCPS staff on the incident team will be informed to keep all details confidential to ensure the investigation and law enforcement efforts are not compromised. The Superintendent will apprise the Board of Education (Board) within 30 days of the validation of the breach and provide ongoing status updates throughout the investigation. An individual who has access to information will be identified and will be provided a non-disclosure agreement to sign and file accordingly per incident. (Form located at http://insidefcps.fcps.org/security)

E. Notification Protocol

The following procedure, as outlined in Maryland law, State Government, §10-1305 shall be followed:

1) Investigation Following Notice of Breach

If FCPS staff discovers, or is notified of a breach of the security of a system, information will be provided to the Director of Technology Infrastructure who shall conduct, in good faith, a reasonable and prompt investigation to determine whether the unauthorized acquisition of personal information of the individual has resulted in or is likely to result in the misuse of the information.

Except as provided below, if after the investigation is concluded, the Director of Technology Infrastructure determines that the misuse of the individual's personal information has occurred or is likely to occur, the Director of Technology Infrastructure shall coordinate efforts to notify the individual of the breach.

2) Permissible Delay of Notification of Breach

The notification required under this section may be delayed:

(a) If a law enforcement agency determines that the notification will impede a criminal investigation or jeopardize homeland or national security; or

(b) To determine the scope of the breach of the security of a system, identify the individuals affected, or restore the integrity of the system.

3) Methods for Notifications

The notification required under this section may be given by written notice sent to the most recent address of the individual in the records of FCPS.

4) Contents of Notification

Unless otherwise prohibited under E.2, notification will be made to affected individuals within 30-45 days of the validation of the breach. The notification required under this section shall include:

(a) To the extent possible, a description of the categories of information that were, or are reasonably believed to have been, acquired by an unauthorized person, including which of the elements of personal information were, or are reasonably believed to have been, acquired;

(b) Contact information for the unit making the notification, including the unit's address, telephone number, and toll-free telephone number if one is maintained;

(c) The toll-free telephone numbers and addresses for the major consumer reporting agencies; and

(d) (i) The toll-free telephone numbers, addresses, and Web site addresses for:
1. the Federal Trade Commission; and
2. the Office of the Attorney General; and
(ii) A statement that an individual can obtain information from these sources about steps the individual can take to avoid identity theft.

(e) The Board will evaluate offering a service of credit monitoring/identity consultation and restoration to individuals who have been identified as victims of data breach within the school system.

5) Required Notification to Office of Attorney General

Before giving the notification required under this section, FCPS shall provide notice of a breach of the security of a system to the Office of the Attorney General.

In addition to the notice required under this section, FCPS, as defined in §10-1301(f)(1) of the State Government Article, shall provide notice of a breach of security to the Department of Information Technology.

6) FERPA Requirements

Maryland law as referenced above has specific notification requirements. The Family Educational Rights and Privacy Act (FERPA) does not require an educational agency to notify students that information from their education records was subject to an unauthorized release. However, it does require the agency to maintain a record of the disclosure. [34CFR99.32(a)(1)]

APPROVED:

Original signed by

Theresa R. Alban
Superintendent