HOBOKEN BOARD OF EDUCATION
OFFICE OF THE SUPERINTENDENT OF SCHOOLS
158 Fourth Street ❖ Hoboken, NJ 07030 ❖ 201.356.3601 ❖ Fax: 201.356.3641

Dr. Christine A. Johnson
Superintendent of Schools
Christine.Johnson@hoboken.k12.nj.us

Data Breach Procedure

1. A data breach generally refers to the unauthorised access and retrieval of information that may include corporate and personal data. Managing data breaches is important to protect the personal data of our clients and their employees when a data breach occurs.

2. Data breaches can occur for different reasons. They may be caused by employees, external vendors or contractors or computer system errors. A data breach could occur in many ways including the following:

Human error:
- Loss of laptop, phone, data storage devices or paper records containing student or staff personal data;
- Sending student or staff personal data to an incorrect e-mail or physical address, or disclosing data to an improper recipient;
- Unauthorized access or disclosure of student or staff personal data by employees;
- Improper disposal of student or staff personal data (e.g. hard disk, storage media or paper documents containing student or staff personal data.

Malicious activities:
- Hacking incidents / illegal access to databases containing student or staff personal data;
- Theft of laptop, phone, data storage devices or paper records containing student or staff personal data;
- Scams that trick organizations into releasing student or staff personal data;

Computer system error:
- Errors or bugs in the programming code of websites, databases and other software which may be exploited to gain access to student or staff personal data stored on computer systems.

3. Data Breach Management Plan
In the event that a data breach happens, the following breach management plan is strictly adhered to. There are five steps to this breach management plan:

I. Identification and classification
II. Containment and recovery
III. Risk assessment
IV. Reporting of breach
V. Evaluation of the response & recovery to prevent future breaches

I. Identification and classification
When a data breach occurs, this should be immediately reported by contacting the building principal and the lead district technician with the information outlined below:

Details of the breach, such as:

- Date;
- Time;
- Who/what reported the breach;
- Description of the breach;
- Details of any IT systems involved, along with corroborating material such as error messages, log files, etc.
- An account of immediate actions taken;

II. Containment and recovery

Once a breach has been reported, the IT Department staff, under the direction of the lead district technician will contain and recover data:

- Shut down the compromised system that led to the data breach and prevent further unauthorized access to the system;
- Reset passwords if accounts and passwords have been compromised;
- Establish whether steps can be taken to recover lost data and limit any damage caused by the breach (e.g. remotely disabling a lost laptop containing personal data of students or staff);
- Isolate the causes of the data breach in the system, and where applicable, change the access rights to the compromised system and remove external connections to the system;
- Notify the police if criminal activity is suspected and preserve evidence for investigation (e.g. hacking, theft or unauthorized system access by an employee);
- Put a stop to practices that led to the data breach;
- Address gaps in processes that led to the data breach.

III. Risk assessment

Knowing the risks and impact of the data breach will help to determine the consequences to affected individuals, as well as the steps necessary to notify the individuals affected. For each data breach, the IT Department will assess:

- How many people were affected?
- Whose personal data has been breached and who might gain access to it?
- To whom does the personal data belong? (e.g. students, staff , contractors, vendors or other third parties)
- What types of personal data were involved?
- How sensitive is the information?
- Do any additional measures have to be put in place to minimise the impact of the data breach?
- What caused the data breach?
- Who needs to be notified?

IV. Reporting of breach

We will notify individuals whose personal data may have been compromised. We will notify other third parties such as the police, where relevant.

We notify affected individuals immediately if a data breach involves sensitive personal data. This allows them to take necessary actions early to avoid potential abuse of the compromised data;

We will notify affected groups and/or individuals in the most effective way, taking into consideration the urgency of the situation and number of individuals affected (e.g. e-mails, telephone calls, letters).

Notifications will be simple to understand, specific and provide clear instructions on what individuals can do to protect themselves.
We will state how and when the data breach occurred, types of personal data involved in the data breach, and what we have done in response to the risks.

.

V. Evaluation of the response & recovery

After these steps have been taken to resolve the data breach, the cause of the breach has to be reviewed and it has to be evaluated whether existing protection and prevention measures are sufficient to prevent similar breaches from occurring.

We will assess whether:

- There are processes that can be streamlined or introduced to limit the damage if future breaches happen or to prevent a relapse;
- There were weaknesses in existing security measures and protection measures, or weaknesses in the use of portable storage devices or connectivity to the Internet;
- The methods for accessing and transmitting personal data were sufficiently secure;
- There is a need to develop new data-breach scenarios;
- Employees were aware of security related issues;
- Training was provided on personal data protection matters and incident management skills;
- There was a clear line of responsibility and communication during the management of the data breach.

CERTIFIED RESOLUTION

9. ACTION - GOVERNANCE AND PERSONNEL

Subject	**9.31 Approval of HPSD Data Breach Procedure for Future Ready Schools**
Meeting	May 14, 2019 - AGENDA
Type	Action (Consent)
Recommended Action	RESOLVED, that the Board of Education, upon recommendation of the Superintendent, approves the district's Data Breach Procedures, as required documentation for the Future Ready Schools certification process and a representation of best-practice.

Motion & Voting

RESOLVED, that the Board of Education approves a Consent Agenda.

Motion by Melanie Tekirian, second by Chetali Khanna.
Final Resolution: Motion Carries
Yes: Malani Cademartori, Sheillah Dallara, Jennifer Evans, Ailene McGuirk, Chetali Khanna, Thomas Kluepfel, Melanie Tekirian, Sharyn Angley

The above is a true copy of a resolution approved by the Hoboken Board of Education at its Public Meeting held on May 14, 2019.

(Signature)
Matthew Boulding, Business Administrator / Board Secretary