BUSINESS & NONINSTRUCTIONAL OPERATIONS

Information Security Breach and Notification

The Board of Education acknowledges the State's concern regarding the rise in identity theft and the need for prompt notification when security breaches occur. To this end, the Board directs the Superintendent, in accordance with appropriate business and technology personnel, to establish regulations which:

- identify and/or define the types of private information that is to be kept secure - for purposes of this policy, "private information" does not include information that can lawfully be made available to the general public pursuant to federal or state law or regulation;

- include procedures to identify any breaches of security that result in the release of private information; and

- include procedures to notify persons affected by the security breach as required by law;

and to conduct an inventory of the District's computer programs and electronic files to determine the types of personal and private information that are maintained by the District. The Superintendent's designee(s) also shall review the safeguards currently in effect to keep such information secure and shall notify the Superintendent and the Board of Education in writing of any additional security precautions recommended to protect such information.

Any breach of the District's computerized data which compromises the security, confidentiality, or integrity of personal and/or private information maintained by the District shall be promptly reported to the Superintendent and the Board of Education.

Legal Reference: State Technology Law §208

Policy Adopted: 3/20/17

WHITE PLAINS CITY SCHOOL DISTRICT
White Plains, New York

BUSINESS & NONINSTRUCTIONAL OPERATIONS

Information Security Breach and Notification Regulations and Procedures

Definitions

Data – Any information created, stored (in temporary or permanent form), filed, produced or reproduced, regardless of the form of the media. Data may include but is not limited to personally identifying information, reports, files, folders, memoranda, statements, examinations, transcripts, images, communications, electronic or hard copy.

Encryption – The cryptographic transformation of data to render it unintelligible through an algorithmic process using a cryptographic key.

Personal information – Any information concerning a natural person which, because of name, number, personal mark or other identifier, can be used to identify such natural person.

Private information – Means 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:

- Social security number;
- Driver's license number or non-driver identification card number or;
- 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.

Note: "Private information" does not include publicly available information that is lawfully made available to the general public pursuant to state or federal law or regulation.

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 and/or private information maintained by the District. Good faith acquisition of personal and/or private information by an officer or employee or agent of the District for the purposes of the District is not a breach of the security of the system, provided that the personal and/or private information is not used or subject to unauthorized disclosure.

1. Procedure for Identifying Security Breaches

In determining whether personal and/or private information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person or a person without valid authorization, the District shall consider:

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; and
4. any other factors which the District shall deem appropriate and relevant to such determination.

2. Security Breaches – Procedures and Methods for Notification to affected persons

Once it has reasonably been determined that a security breach has occurred, the following steps shall be taken:

A. Where computerized data is owned or licensed by the District

If the breach or suspected breach involved computerized data owned or licensed by the District, the District shall notify those New York State residents whose *personal and/or private information* was, or is reasonably believed to have been, acquired by a person without valid authorization. The disclosure to such persons shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement (as explained in **3** below) and consistent with the District's need to take measures to determine the scope of the breach and to restore the reasonable integrity of the data system. In this regard, the District may consult with the New York State Office of Information and Technology Services to determine the scope of the breach and the appropriate restoration measures.

B. Where computerized data is maintained by the District

Where a breach or suspected breach of involves computerized data that is maintained by the District**,** the District shall notify the owner or licensee of the information of the breach of the security of the system immediately following discovery, if personal and/or private information was -- or is reasonably believed to have been -- acquired by a person without valid authorization.

C. Contents of the Notice

The notice provided by the District shall include (a) district contact information, (b) a description of the categories of information that were or are reasonably believed to have been acquired without authorization and (c) which specific elements of personal or private information were or are reasonably believed to have been acquired.

D. Acceptable Methods of Giving Notice

Notice shall be directly provided to the affected individuals by one of the following methods:

- Written notice
- Electronic notice, provided that the person to whom notice is required has expressly consented to receiving the notice in electronic form; and that the District keeps a log of each such electronic notification. In no case, however, shall the District require a person to consent to accepting such notice in electronic form as a condition of establishing a business relationship or engaging in any transaction with the District.
- Telephone notification, provided that the District keeps a log of each such telephone notification.
- Substitute Notice - If the District can demonstrate to the State Attorney General that (a) the cost of providing notice would exceed $250,000; or (b) that the number of persons to be notified exceeds 500,000 or (c) that the District does not have sufficient contact information, substitute notice may be provided. Substitute notice would consist of all of the following steps:

  a. E-mail notice when the District has such address for the affected individual;
  b. Conspicuous posting on the District's website, if it maintains one; and
  c. Notification to major media in the area(s) of the affected individuals.

3. Delayed Notification in Cooperation with Law Enforcement

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

4. Notification of State and Other Agencies

Once notice has been made to affected New York State residents, the District shall notify the State Attorney General, the New York State Department of State, and the New York State Office of Information and Technology Services as to the timing, content, and distribution of the notices and approximate number of affected persons.

If more than 5,000 New York State residents are to be notified at one time, the District shall also notify consumer reporting agencies as to the timing, content and distribution of the notices and the approximate number of affected individuals. A list of consumer reporting agencies will be furnished, upon request, by the Office of the State Attorney General.

Regulations Adopted: 3/20/17

WHITE PLAINS CITY SCHOOL DISTRICT
White Plains, New York

INFORMATION SECURITY BREACH AND NOTIFICATION REGULATION AND PROCEDURES

Definitions

Data – Any information created, stored (in temporary or permanent form), filed, produced or reproduced, regardless of the form of the media. Data may include but is not limited to personally identifying information, reports, files, folders, memoranda, statements, examinations, transcripts, images, communications, electronic or hard copy.

Encryption – The cryptographic transformation of data to render it unintelligible through an algorithmic process using a cryptographic key.

Personal information – Any information concerning a natural person which, because of name, number, personal mark or other identifier, can be used to identify such natural person.

Private information – Means 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:

- Social security number;
- Driver's license number or non-driver identification card number or;
- 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.

Note: "Private information" does not include publicly available information that is lawfully made available to the general public pursuant to state or federal law or regulation.

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 and/or private information maintained by the District. Good faith acquisition of personal and/or private information by an officer or employee or agent of the District for the purposes of the District is not a breach of the security of the system, provided that the personal and/or private information is not used or subject to unauthorized disclosure.

Regulation 8635-R

1. Procedure for Identifying Security Breaches

In determining whether personal and/or private information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person or a person without valid authorization, the District shall consider:

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; and
4. any other factors which the District shall deem appropriate and relevant to such determination.

2. Security Breaches – Procedures and Methods for Notification to affected persons

Once it has reasonably been determined that a security breach has occurred, the following steps shall be taken:

A. Where computerized data is owned or licensed by the District

If the breach or suspected breach involved computerized data owned or licensed by the District, the District shall notify those New York State residents whose *personal and/or private information* was, or is reasonably believed to have been, acquired by a person without valid authorization. The disclosure to such persons shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement (as explained in **3** below) and consistent with the District's need to take measures to determine the scope of the breach and to restore the reasonable integrity of the data system. In this regard, the District may consult with the New York State Office of Information and Technology Services to determine the scope of the breach and the appropriate restoration measures.

B. Where computerized data is maintained by the District

Where a breach or suspected breach of involves computerized data that is maintained by the District**,** the District shall notify the owner or licensee of the information of the breach of the security of the system immediately following discovery, if personal and/or private information was -- or is reasonably believed to have been -- acquired by a person without valid authorization.

C. Contents of the Notice

The notice provided by the District shall include (a) district contact information, (b) a description of the categories of information that were or are reasonably believed to have been acquired without authorization and (c) which specific elements of personal or private information were or are reasonably believed to have been acquired.

D. Acceptable Methods of Giving Notice

Notice shall be directly provided to the affected individuals by one of the following methods:

- Written notice
- Electronic notice, provided that the person to whom notice is required has expressly consented to receiving the notice in electronic form; and that the District keeps a log of each such electronic notification. In no case, however, shall the District require a person to consent to accepting such notice in electronic form as a condition of establishing a business relationship or engaging in any transaction with the District.
- Telephone notification, provided that the District keeps a log of each such telephone notification.
- Substitute Notice - If the District can demonstrate to the State Attorney General that (a) the cost of providing notice would exceed $250,000; or (b) that the number of persons to be notified exceeds 500,000 or (c) that the District does not have sufficient contact information, substitute notice may be provided. Substitute notice would consist of all of the following steps:

  a. E-mail notice when the District has such address for the affected individual;
  b. Conspicuous posting on the District's website, if it maintains one; and
  c. Notification to major media in the area(s) of the affected individuals.

3. Delayed Notification in Cooperation with Law Enforcement

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

4. Notification of State and Other Agencies

Once notice has been made to affected New York State residents, the District shall notify the State Attorney General, the New York State Department of State, and the New York State Office of Information and Technology Services as to the timing, content, and distribution of the notices and approximate number of affected persons.

If more than 5,000 New York State residents are to be notified at one time, the District shall also notify consumer reporting agencies as to the timing, content and distribution of the notices and the approximate number of affected individuals. A list of consumer reporting agencies will be furnished, upon request, by the Office of the State Attorney General.

Adoption date: