Non-Instructional/Business Operations

SUBJECT: DISPOSAL OF CONSUMER REPORT INFORMATION AND RECORDS

In accordance with the Federal Trade Commission's (FTC) "Disposal Rule," and in an effort to protect the privacy of consumer information, reduce the risk of fraud and identity theft, and guard against unauthorized access to or use of the information, the District will take appropriate measures to properly dispose of sensitive information (i.e., personal identifiers) contained in or derived from consumer reports and records. The District may determine what measures are reasonable based on the sensitivity of the information, the costs and benefits of different disposal methods, and changes in technology.

The term "consumer report" includes information obtained from a consumer reporting company that is used—or expected to be used—in establishing a consumer's eligibility for employment or insurance, among other purposes. The term "employment purposes" when used in connection with a consumer report means a report used for the purpose of evaluating a consumer for employment, promotion, reassignment, or retention as an employee.

The FTC Disposal Rule defines "consumer information" as "any record about an individual, whether in paper, electronic, or other form, that is a consumer report or is derived from a consumer report. Consumer information also means a compilation of these records. Consumer information does not include information that does not identify individuals, such as aggregate information or blind data."

Information Covered by the Disposal Rule

There are a variety of personal identifiers beyond simply a person's name that would bring information within the scope of the Disposal Rule, including, but not limited to, a social security number, driver's license number, phone number, physical address, and email address. Depending upon the circumstances, data elements that are not inherently identifying can, in combination, identify particular individuals.

Proper Disposal

The District will utilize disposal practices that are reasonable and appropriate to prevent the unauthorized access to—or use of—information contained in or derived from consumer reports and records. Reasonable measures to protect against unauthorized access to or use of consumer information in connection with District disposal include the following examples.

a) Burning, pulverizing, or shredding of papers containing consumer information so that the information cannot practicably be read or reconstructed;

b) Destroying or erasing electronic media containing consumer information so that the information cannot practicably be read or reconstructed;

(Continued)

SUBJECT: DISPOSAL OF CONSUMER REPORT INFORMATION AND RECORDS (Cont'd.)

c) After due diligence, entering into and monitoring compliance with a contract with another party engaged in the business of record destruction to dispose of material, specifically identified as consumer information, in a manner consistent with the Disposal Rule. In this context, due diligence could include:

1. Reviewing an independent audit of the disposal company's operations and/or its compliance with the Disposal Rule;

2. Obtaining information about the disposal company from several references or other reliable sources;

3. Requiring that the disposal company be certified by a recognized trade association or similar third party;

4. Reviewing and evaluating the disposal company's information security policies or procedures;

5. Taking other appropriate measures to determine the competency and integrity of the potential disposal company; or

6. Requiring that the disposal company have a certificate of registration from the New York Department of State issued on or after October 1, 2008.

d) For persons (as defined in accordance with the Fair Credit Reporting Act) or entities who maintain or otherwise possess consumer information through their provision of services directly to a person subject to the Disposal Rule, monitoring compliance with policies and procedures that protect against unauthorized or unintentional disposal of consumer information, and disposing of this information in accordance with examples a) and b) above.

Implementation of Practices and Procedures

The Board delegates to the Superintendent or designee the authority and responsibility to review current practices regarding the disposal of consumer information; and to implement such further reasonable and appropriate procedures, including staff training as necessary, to ensure compliance with the FTC's Disposal Rule.

The Fair Credit Reporting Act, 15 USC § 1681 et seq.
The Fair and Accurate Credit Transactions Act of 2003, Public Law §§ 108-159
Federal Trade Commission Disposal of Consumer Report Information and Records, 16 CFR Part 682
General Business Law Article 39-G
19 NYCRR § 199

Adopted: 1/14/21

Non-Instructional/Business Operations

SUBJECT: INFORMATION SECURITY BREACH AND NOTIFICATION

The District values the protection of private information of individuals in accordance with applicable law and regulations. The District is required to notify affected individuals when there has been or is reasonably believed to have been a compromise of the individual's private information in compliance with the Information Security Breach and Notification Act and Board policy.

a) "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:

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

b) "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 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.

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:

a) Indications that the information is in the physical possession or control of an unauthorized person, such as a lost or stolen computer or other device containing information;

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

(Continued)

SUBJECT: INFORMATION SECURITY BREACH AND NOTIFICATION (Cont'd.)

c) Indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported; or

d) System failures.

Notification Requirements

a) For any computerized data owned or licensed by the District that includes private information, the District will disclose any breach of the security of the system following discovery or notification of the breach to any New York State resident whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization. The disclosure to affected individuals will be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. The District will consult with the State Office of Information Technology Services to determine the scope of the breach and restoration measures.

b) For any computerized data maintained by the District that includes private information which the District does not own, the District will notify the owner or licensee of the information of any breach of the security of the system immediately following discovery, if the private information was, or is reasonably believed to have been, acquired by a person without valid authorization.

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

Methods of Notification

The required notice will be directly provided to the affected persons by one of the following methods:

a) Written notice;

b) 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 will 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;

c) Telephone notification, provided that a log of each notification is kept by the District when notifying affected persons by phone; or

(Continued)

SUBJECT: INFORMATION SECURITY BREACH AND NOTIFICATION (Cont'd.)

d) 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 will consist of all of the following:

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

2. Conspicuous posting of the notice on the District's website page, if the District maintains one; and

3. Notification to major statewide media.

Regardless of the method by which notice is provided, the notice will include contact information for the notifying District and a description of the categories of information that were, or are reasonably believed to have been, acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so acquired.

In the event that any New York State residents are to be notified, the District will notify the New York State Attorney General (AG), the New York State Department of State, and the New York State Office of Information Technology Services as to the timing, content, and distribution of the notices and approximate number of affected persons.

In the event that more than 5,000 New York State residents are to be notified at one time, the District will also notify consumer reporting agencies, as defined in State Technology Law Section 208, as to the timing, content, and distribution of the notices and approximate number of affected persons. This notice will be made without delaying notice to affected New York State residents. A list of consumer reporting agencies will be compiled by the AG and furnished upon request to school districts required to make a notification in accordance with State Technology Law Section 208(2), regarding notification of breach of security of the system for any computerized data owned or licensed by the District that includes private information.

State Technology Law §§ 202 and 208

Adopted: 1/14/21