TECHNOLOGY SECURITY FOR PERSONAL, PRIVATE AND SENSITIVE INFORMATION

SUBJECT: EMPLOYEE PERSONAL IDENTIFYING INFORMATION

In accordance with Section 203-d of the New York State Labor Law, the District shall restrict the use and access to employee personal identifying information. As enumerated in law, "personal identifying information" shall include social security number, home address or telephone number, personal electronic mail address, Internet identification name or password, parent's surname prior to marriage, driver's license number, or other information designated as Private Information under the District's Information Security Breach Notification Regulation.

The District shall not unless otherwise required by law:

a) Publicly post or display an employee's social security number;
b) Visibly print a social security number on any identification badge or card, including any time card;
c) Place a social security number in files with unrestricted access; or
d) Communicate an employee's personal identifying information to the general public.

A social security number shall not be used as an identification number for purposes of any occupational licensing.

District staff shall have access to this policy, informing them of their rights and responsibilities in accordance with Labor Law Section 203-d. District procedures for safeguarding employee "personal identifying information" shall be evaluated; and employees who have access to such information as part of their job responsibilities shall be advised as to the restrictions on release of such information in accordance with law.

Data Sensitivity

a) For the purpose of this regulation, "sensitive data" is considered any and all student and employee data which is considered personal, private and sensitive information (PPSI) or any non PPSI information which assembled together would allow a reasonable person to identify an individual. Sensitive data includes, but is not limited to:

    1. Student personally identifiable information, except as allowed by the Family Educational Rights and Privacy Act (20 U.S.C. § 1232g; 34 CFR Part 99);

    2. Social Security Number;

    3. Driver's License Number or non-drivers card number;

4. Account number, credit or debit, in combination with any required security code, access code, or password which would permit access to an individual's financial account;

5. All of "personally identifiable information" of students, teachers, and District employees under Education Law §2-d and Part 121 of the regulations of the Commissioner of Education

SUBJECT: TECHNOLOGY SECURITY MANAGEMENT

Sensitive Data

Data Sensitivity

b) For the purpose of this regulation, "sensitive data" is considered any and all student and employee data which is considered personal, private and sensitive information (PPSI) or any non PPSI information which assembled together would allow a reasonable person to identify an individual. Sensitive data includes, but is not limited to:

1. Student personally identifiable information, except as allowed by the Family Educational Rights and Privacy Act (20 U.S.C. § 1232g; 34 CFR Part 99);

2. Social Security Number;

3. Driver's License Number or non-drivers card number;

4. Account number, credit or debit, in combination with any required security code, access code, or password which would permit access to an individual's financial account;

5. All of "personally identifiable information" of students, teachers, and District employees under Education Law §2-d and Part 121 of the regulations of the Commissioner of Education

All the above information should be stored only on district approved information management systems that are password protected with access limited by users' rights. The District shall not sell nor use or disclose any of the above information for marketing or commercial purposes or permit or facilitate another party to use or disclose any of the above information for marketing or commercial purposes. The District shall take steps to minimize the collection, processing and transmission of sensitive data.

c) District employees having access to sensitive information shall receive annual training which emphasizes their personal responsibility for protecting student and employee information, including compliance training on all state and federal laws that protect personally identifiable information.

d) Private information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

e) Personal information shall mean any information concerning a person which, because of name, number, symbol, mark, or other identifier, can be used to identify that person.

f) All employees should be aware that inclusion of PPSI in email correspondence possesses a security risk. Every effort should be made to limit the amount of PPSI information included in email to that necessary to reasonably conduct district business.

Workstation Security

a) District shall ensure that user workstations must not be left unattended when logged into sensitive systems or data including student or employee information. Workstations will lock after a period of inactivity.

District shall ensure that all equipment that contains sensitive information will be secured to deter theft. All District employees that are issued devices that can be used remotely will be trained annually on how to safeguard sensitive data.

Computer Room Security

The District shall ensure that server rooms and telecommunication rooms/closets are protected by appropriate access control which segregates and restricts access from general school or District office areas. The District shall ensure that the network operations and back up location, is protected by appropriate access control.

SUBJECT: INFORMATION SECURITY MANAGEMENT

The District values the protection of private information of individuals in accordance with applicable law and regulations, and best practice. Therefore, District management and Information Technology (IT) staff will plan, deploy, and monitor IT security mechanisms, policies, procedures, and technologies necessary to prevent disclosure, modification, or denial of sensitive information. The District adopts the National Institute for Standards and Technology

Technology Security for Personal, Private and Sensitive Information
Information Security Management (Continued)

Cybersecurity Framework as their standard for data security and protection. The District has designated a Data Protection Officer that has appropriate knowledge, training and experience to be responsible for implementation of data security policies required by Education Law §2-d and Part 121 of the Regulations of the Commissioner of Education.

Therefore, the Data Protection Officer in collaboration with the Technology Department, shall:

a) Inventory and classify Personal, Private, and Sensitive Information (PPSI) on its systems to protect the confidentiality, integrity, and availability of information;

b) Control physical access to computer facilities, data rooms, systems, networks and data to those authorized personnel who require access to perform assigned duties;

c) Implement network perimeter controls to regulate traffic moving between trusted internal (District) resources and external, untrusted (internet) entities;

d) Grant access to systems and applications based upon the least amount of access to data and programs required by the user in accordance with a business need-to-have requirement;

e) Develop a business continuity/disaster recovery plan appropriate for the size and complexity of District IT operations to ensure continuous critical IT services;

f) Deploy to servers and workstations software to identify and eradicate malicious software attacks such as viruses and malware;

g) Ensure that every use and disclosure of personally identifiable information benefits the students and the District;

h) Ensure that personally identifiable information is not included in any public reports; and

i) Ensure that the District's systems follow NIST CFS and that all technologies, safeguards and practices at a minimum meet the NIST CFS standard.

Technology Security for Personal, Private and Sensitive Information

SUBJECT: THIRD PARTY CONTRACTORS

The District will ensure that contracts involving the disclosure of personally identifiable information with third-party contractors or separate data sharing and confidentiality agreements require the confidentiality of shared personally identifiable information be maintained in accordance with federal and state law and the District's data security and privacy policy. Additionally, all such contracts entered into with third-party contractors must include a data security and privacy plan that conforms with federal and state law, including Education Law §2-d and Part 121 of the Regulations of the Commissioner of Education, and all contracts must include a signed copy of the Parents' Bill of Rights (Exhibit 3802-E).

In accordance with Education Law § 2-d(5)(b)(1) and Section 121.5 of the Regulations of the Commissioner of Education, disclosure of personally identifiable information from the student records of the District, including directory information, to individuals or entities other than the parent/guardian or eligible student or which is not otherwise permitted by applicable consent or provision of Education Law § 2-d, shall be predicated upon a determination that the proposed use would benefit students and the District (e.g., improve academic achievement, empower parents and students with information, and/or advance efficient and effective school operations).

Adopted:
April 23, 2018
Revised:
June 29, 2020
Revised:
March 21, 2022
Revised:
August 21, 2023
Reviewed:
September 16, 2024