Data

Data Governance

Purpose

It is the District's policy to the extent possible to ensure that data and information in all its forms, written, electronic or printed is protected from accidental or intentional unauthorized modification, destruction or disclosure. The protection includes an appropriate level of security over the equipment, software and practices used to process, store and transmit data or information.

Data Security Administrator and Data Governance Committee

The District's superintendent will designate a District employee to serve as the Data Security Administrator. The Data Security Administrator will be responsible for overseeing the implementation of the District's security policies and procedures. The Data Security Administrator will also select District employees to serve on the District's Data Governance Committee. This Committee will be responsible for an annual review of all data governance policies and procedures.

Further, the Data Security Administrator and the Data Governance Committee will assist the District administration in implementing a comprehensive annual training program on the District's data policies.

Regulatory Compliance

The District will comply with applicable law, regulations or contractual obligations which affects its data systems including, but not limited to:

1. Children's Internet Protection Act (CIPA);
2. Children's On-Line Privacy Protection Act (COPPA);
3. Family Educational Rights and Privacy Act (FERPA); and
4. Protection of Pupil Rights Act (PPRA).

Risk Analysis

Annually, and as requested by the Superintendent, a thorough risk analysis of the District's data networks, systems, policies and procedures will be conducted. The risk assessment will be used as a basis for a plan to minimize identified risks.

Data Classification

Data is classified according to the most sensitive detail which they include. The classification assigned and the related controls applied are dependent on the sensitivity of the data.

Systems and Information Control

Any computer, laptop, model device, preliminary and/or screening device, network, appliance/equipment, AV equipment, server, internal or external storage, communication device or any other current or future electronic device may be referred to as "systems." All involved systems and information are assets of the District and shall be protected from misuse, unauthorized manipulation and destruction. These protection measures may be physical and/or software based.

Ownership of Software

All computer software developed by the District employees or contract personnel on behalf of the District, licensed or purchased for the District's use is the property of the District and shall not be copied for use at home or any other location, unless otherwise specified by the license agreement.

Software Installation and Use

All software packages that reside on technological systems within or used by the District shall comply with applicable licensing agreements and restrictions and shall comply with the District's acquisition of software procedures.

Virus, Malware, Spyware, Phishing and SPAM Protection

Virus checking systems approved by the District Technology Department are deployed using a multi-layered approach (computers, servers, gateways, firewalls, filters, etc.) that ensures all electronic files are appropriately scanned for viruses, malware, spyware, phishing and SPAM. Users shall not turn off or disable the District's protection systems or to install other systems.

Access Controls

Physical and electronic access to information systems that contain Personally Identifiable Information (PII), Confidential Information, Internal Information and computing resources shall be controlled. To ensure appropriate levels of access by District employees, a variety of security measures are instituted as recommended by the data governance committee and approved by the District. In particular, the data governance committee shall document roles and rights to the student information system and other like systems. Mechanisms to control access to PII, Confidential Information, Internal Information and computing resources include, but are not limited to, the following methods:

1. Authorization: Access shall be granted on a "need to know" basis and shall be authorized by the superintendent, principal, immediate supervisor, or Data Governance Committee with the assistance of the Technology Director and/or Data Security Officer. Specifically,

on a case-by-case basis, permissions may be added in to those already held by individual users in the student management system, again on a need-to-know basis and only in order to fulfill specific job responsibilities, with approval of the Data Governance Committee.

2. Identification/Authentication: Unique user identification (user ID) and authentication are required for all systems that maintain or access PII, Confidential information, and/or Internal Information. Users shall be held accountable for all actions performed on the system with their User ID. User accounts and passwords shall NOT be shared.

3. Data Integrity: The District provides safeguards so that PII, Confidential, and Internal Information is not altered or destroyed in an unauthorized manner. Core data are backed up to a private cloud for disaster recovery. In addition, listed below are methods that are used for data integrity in various circumstances:

    a) transaction audit;

    b) disk redundancy (RAID);

    c) ECC (Error Correcting Memory);

    d) checksums (file integrity);

    e) data encryption;

    f) data wipes.

4. Transmission Security: Technical security mechanisms are in place to guard against unauthorized access to data that are transmitted over a communications network, including wireless networks. The following features are implemented:

    a) integrity controls; and

    b) encryption, where deemed appropriate.

5. Remote Access: Access into the District's network from outside is allowed using the District's Portal. All other network access options are strictly prohibited without explicit authorization from the Technology Director, ISO, or Data Governance Committee. Further, PII, Confidential Information and/or Internal Information that is stored or accessed remotely shall maintain the same level of protections as information stored and accessed within the District's network. PII shall only be stored in cloud storage if said storage has been approved by the Data Governance Committee or its designees.

6. Physical and Electronic Access and Security: Access to areas in which information processing is carried out shall be restricted to only appropriately authorized individuals. At a minimum, staff passwords shall be changed annually.

a) No PII, Confidential and/or Internal Information shall be stored on a device itself such as a hard drive, mobile device of any kind, or external storage device that is not located within a secure area or password protected.

b) No technological systems that may contain information as defined above shall be disposed of or moved without adhering to the appropriate Purchasing and Disposal of Electronic Equipment procedures.

c) It is the responsibility of the user to not leave these devices logged in, unattended, and open to unauthorized use.

7. Inactive Accounts and Terminated Users: User accounts and related access privileges shall be terminated promptly at the end of an employee's employment. The District's administrative team will inform the Data Governance Committee when an employee's employment has ended or will end in the future in order to facilitate account closure. Further, user access rights shall be reviewed periodically to determine if and when access rights are no longer necessary for certain District employees.

Data Transfer/Exchange/Printing

Electronic Mass Data Transfers: Downloading, uploading or transferring PII, Confidential Information, and Internal Information between systems shall be strictly controlled. Requests for mass download of, or individual requests for, information for research or any other purposes that include PII shall be in accordance with this policy and be approved by the Data Governance Committee. All other mass downloads of information shall be approved by the Committee and/or Data Security Administrator and include only the minimum amount of information necessary to fulfill the request. At the very least, a Memorandum of Agreement (MOA) shall be in place when transferring PII to third party entities such as software or application vendors, textbook companies, testing companies, or any other web based application, etc. unless the exception is approved by the Data Governance Committee. Further, the Data Governance Committee is responsible for ensuring that any MOAs or agreements with third party entities in possession of District data comply with the Federal regulations identified in this regulation.

Other Electronic Data Transfers and Printing: PII, Confidential Information, and Internal Information shall be stored in a manner inaccessible to unauthorized individuals. PII and Confidential Information shall not be downloaded, copied or printed indiscriminately or left unattended and open to compromise. PII that is downloaded for educational purposes where possible shall be de-identified before use.

Oral Communications: The District's staff shall be aware of their surroundings when discussing PII and Confidential Information. This includes but is not limited to the use of cellular telephones in public areas. The District's staff shall not discuss PII or Confidential Information in public areas if the information can be overheard. Caution shall be used when conducting conversations in: semi-private rooms, waiting rooms, corridors, elevators, stairwells, cafeterias, restaurants, or on public transportation.

Audit Controls: Hardware, software, services and/or procedural mechanisms that record and examine activity in information systems that contain or use PII are reviewed by the Data Governance Committee annually. Further, the committee also regularly reviews records of information system activity, such as audit logs, access reports, and security incident tracking reports. These reviews shall be documented and maintained for six (6) years.

Evaluation: The District will require that periodic technical and non-technical evaluations of access controls, storage, and other systems be performed in response to environmental or operational changes affecting the security of electronic PII to ensure its continued protection.

IT Disaster Recovery: Controls shall ensure the District can recover from any damage to critical systems, data, or information within a reasonable period of time. Each school, department, or individual is required to report any instances immediately to the Superintendent, Data Security Administrator, and/or Technology Director for response to a system emergency or other occurrence (for example, fire, vandalism, system failure and natural disaster) that damages data or systems. The IT Disaster Plan shall include the following:

1. A prioritized list of critical services, data, and contacts.

2. A process enabling the District to restore any loss of data in the event of fire, vandalism, natural disaster, or system failure.

3. A process enabling the District to continue to operate in the event of fire, vandalism, natural disaster, or system failure.

4. Procedures for periodic testing of written contingency plans to discover weaknesses and the subsequent process of revising the documentation, if necessary.

Compliance

The Data Governance Policy applies to all users of the District's information including: employees, staff, students, volunteers, and third party vendors. Failure to comply with this policy by employees, staff, volunteers, and third party vendors may result in disciplinary action up to and including dismissal in accordance with applicable the District's procedures, or, in the case of third party vendors, termination of the contractual relationship. Failure to comply with this policy by students may constitute grounds for corrective action in accordance with the District's policies. Further, penalties associated with state and federal laws may apply.

Possible disciplinary/corrective action may be instituted for, but is not limited to, the following:

1. Unauthorized disclosure of PII or Confidential Information.

2. Unauthorized disclosure of a log-in code (User ID and password).

3. An attempt to obtain a log-in code or password that belongs to another person.

4. An attempt to use another person's log-in code or password.

5. Unauthorized use of an authorized password to invade student or employee privacy by examining records or information for which there has been no request for review.

6. Installation or use of unlicensed software on the District's technological systems.

7. The intentional unauthorized altering, destruction, or disposal of the District's information, data and/or systems. This includes the unauthorized removal from the District's technological systems such as but not limited to laptops, internal or external storage, computers, servers, backups or other media, copiers, etc. that contain PII or confidential information.

8. An attempt to gain access to log-in codes for purposes other than for support by authorized technology staff, including the completion of fraudulent documentation to gain access.

****

Board Adopted January 19, 2017
Board Reviewed December 11, 2018