Policy for Ensuring the Security of Private and Confidential Data on Individuals

This policy is required by Minnesota Statutes, section 13.05, subd. 5. The procedures listed below are incorporated to constitute this policy.

Safeguards for Private and Confidential Data on Individuals

Minneapolis Public Schools (MPS) has established the following safeguards:

- Cyber security practices, including but not limited to: password-protected network and information systems; requirement of strong passwords; staff training; multi-factor authentication; and frequent security scans
- The use of locked storage receptacles for physical records containing private and confidential data
- Policies that 1) define private and confidential data on individuals; 2) provide for who may access it; and 3) require it to be securely destroyed when its retention period has been met

Ensuring That Private and Confidential Data on Individuals Are Not Accessed Without a Work Assignment

Data Inventory

Under the requirement in Minnesota Statutes, section 13.025, subd. 1, MPS has prepared a Data Inventory which identifies and describes all private and confidential data on individuals maintained by MPS. To comply with the requirement in section 13.05, subd. 5, MPS has also modified its Data Inventory to represent the employees who have access to private and confidential data on individuals based on their work assignments. In the event of a temporary duty as assigned by a manager or supervisor, an employee may access certain private and confidential data on individuals, for as long as the work is assigned to the employee. In addition to the employees listed the Data Inventory, the Responsible Authority, the Data Practices Compliance Official, Superintendent's Cabinet, and General Counsel may have access to all private and confidential data on individuals maintained by MPS if necessary for specified duties. Any access to private and confidential data on individuals will be strictly limited to the data necessary to complete the work assignment.

Limited Access to Systems/Repositories Containing Private and Confidential Data on Individuals

An employee is allowed access to private and confidential data on individuals only when their work assignment reasonably requires it. An employee must use the applicable request form to request access to systems and repositories that contain private and confidential data on individuals. Requests for access must be reviewed and considered by an employee's supervisor

and the business owner of the system or repository. The supervisor and business owner will approve a request for access only when the employee's work assignment reasonably requires it.

Data Sharing with Authorized Entities or Individuals

State or federal law may authorize the sharing of private and confidential data on individuals in specific circumstances. Private and confidential data on individuals may be shared with another entity if state or federal law allows or mandates it. Individuals will have notice of any sharing in applicable Tennessen warnings (see Minnesota Statutes, section 13.04) or MPS will obtain the individual's informed consent. Any sharing of private and confidential data on individuals will be strictly limited to the data necessary or required to comply with the applicable law.

Penalties for Unlawfully Accessing Private and Confidential Data on Individuals

MPS will impose the penalties for unlawful access to not public data as provided for in Minnesota Statutes, section 13.09, when appropriate. Penalties include suspension, dismissal, or referring the matter to the appropriate prosecutorial authority who may pursue a criminal misdemeanor charge.

(Last reviewed 08/07/2024)