| | |
|---|---|
| Book | Board of Education Policies (NYSSBA) |
| Section | 8000 Instruction |
| Title | DATA PRIVACY AND SECURITY POLICY |
| Code | 8630 |
| Status | Active |
| Adopted | September 15, 2020 |

## I. Purpose

This policy addresses The Mount Vernon City School District's ("MVCSD") responsibility to adopt appropriate administrative, technical and physical safeguards and controls to protect and maintain the confidentiality, integrity and availability of its data (including Private Data), data systems and information technology resources (collectively, "MVCSD Data/Programs").

## II. Policy Statement

It is the policy of MVCSD:

(1) to comply with legal and regulatory requirements governing the collection, retention, dissemination, protection, and destruction of information by, from and as part of the MVCSD Data/Programs;
(2) to maintain a comprehensive Data Privacy and Security Program designed to satisfy its statutory and regulatory obligations, enable and assure core services, and fully support the safety and security of the MVCSD Data/Programs;
(3) to protect personally identifiable information, and sensitive and confidential information ("Private Data") from unauthorized use or disclosure;
(4) to address the adherence of its vendors with federal, state and MVCSD requirements in its vendor agreements involving or accessing Private Data;
(5) to train its users who share a measure of responsibility for protecting the MVCSD Data/Programs; and
(6) to communicate its required data security and privacy responsibilities and the consequences of non-compliance, to its Users.

## III. Standard

The Mount Vernon City School District will utilize the National Institute of Standards and Technology's Cybersecurity Framework v 1.1 (NIST CSF or Framework) as the standard for its Data Privacy and Security Program. Such standard may be updated from time to time to incorporate and accommodate the latest improvements in cybersecurity available to school districts.

## IV. Scope

The policy applies to the Mount Vernon City School District employees, and to independent contractors, interns, volunteers ("Users") and third-party contractors who receive or have access to MVCSD Data/Programs.
This policy encompasses, and the MVCSD Data/Programs include, all systems, automated and manual, including systems managed or hosted by third parties on behalf of MVCSD, and it applies to all data and information, regardless of the form or format, which is created or used in support of the activities of MVCSD.
This policy shall be published on the MVCSD website and notice of its existence shall be provided to all employees and other Users.

## V. Compliance

The Superintendent or their designee shall ensure compliance of this policy, related policies, and their applicable standards, guidelines and procedures. Instances of non-compliance will be addressed on a case-by-case basis. All cases will be documented, and employees and other Users and vendors will be directed to adopt corrective practices, as applicable.

## VI. Oversight

The Superintendent or their designee shall appoint a Data Protection Officer. MVCSD's Data Protection Officer shall annually report to the MVCSD Board and Superintendent on data privacy and security activities and progress, the number and disposition of reported breaches, if any, and a summary of any complaint submitted pursuant to Education Law §2-d. In addition, any critical incidents will be timely reported in accordance with MVCSD's Information Security Breach and Notification Policy #5672.

## VII. Data Privacy

(1) Laws such as the Family Educational Rights Privacy Act (FERPA), NYS Education Law §2-d and other state or federal laws establish baseline parameters for what is permissible when sharing certain Private Data.
(2) Private Data must only be used in accordance with applicable law and regulation and MVCSD policies to ensure it is protected from unauthorized use and/or disclosure.
(3) The Data Protection Officer and applicable staff that manage the use of Private Data will, together with district leaders at the direction of the Superintendent or designee, determine on a case-by-case basis whether a proposed use of elements of Private Data would benefit students and/or educational agencies, and to ensure that personally identifiable information is not included in public reports or other public documents, or otherwise publicly disclosed in violation of law.
(4) No Private Data shall be shared with third parties without a written agreement that complies with state and federal laws and regulations. No Private Data will be provided to third parties unless it is permitted by state and federal laws and regulations. Any third-party contracts relating to Private Data must include provisions required by state and federal laws and regulation.
(5) The identity of all individuals requesting Private Data of a student, even where they claim to be a parent and persons in parental relationships or the student themselves, is subject to authentication in accordance with applicable law and MVCSD policies and procedures.
(6) It is MVCSD's policy to abide by and ensure (and, where MVCSD's responsibility, to provide) all protections in respect of Private Data of students afforded to parents and persons in parental relationships, and students themselves where applicable, to the extent required under the Family Educational Rights and Privacy Act, the Individuals with Disabilities Education Act, and the federal regulations implementing such statutes. Therefore, MVCSD shall require that its contracts require that the confidentiality of Private Data (including teacher or principal APPR data) be maintained in accordance with federal and state law and this policy.
(7) Contracts with third parties that will receive or have access to Private Data must ensure the confidentiality of data is maintained in accordance with state and federal laws and regulations and this policy.

(8) To the extent Private Data includes personal health or medical data, such data shall be retained, managed and disclosed in all respects in accordance with the applicable provisions of HIPAA and other laws and regulations relating to such data.

VIII. **Incident Response and Notification**

The MVCSD will respond to data privacy and security critical incidents in accordance with its Information Security Breach and Notification Policy. All breaches of data and/or data systems part of MVCSD Data/Programs (including, but not limited to, breaches of Private Data) must be reported to the Chief Technology Administrator and Data Protection Officer. For purposes of this policy, a breach means the unauthorized acquisition, access, use, or disclosure of student, teacher or principal PII as defined by Education law §2-d, or any MVCSD sensitive or confidential data or a data system that stores that data, by or to a person not authorized to acquire, access, use, or receive the data. State and federal laws require that affected individuals must be notified when there has been a breach or unauthorized disclosure of personally identifiable information. Upon receiving a report of a breach or unauthorized disclosure, Data Protection Officer, MVCSD's counsel and other subject matter experts will determine whether notification of affected individuals is required, and where required, effect notification in the most expedient way possible and without unreasonable delay. Nothing in this policy shall be construed as a guarantee against, or indemnity on the part of MVCSD for, any breach or damages that may arise from a breach (directly or indirectly), whether such breach was intentional or unintentional, whether arising from a hacking, virus, malware, accident or otherwise.

IX. **Acceptable Use Policy, Password Policy and other Related Department Policies**

(1) Users must comply with the Acceptable Use Policy in using MVCSD Data/Programs. Access privileges to MVCSD Data/Programs will be granted in accordance with the User's job responsibilities and will be limited only to those necessary to accomplish assigned tasks in accordance with MVCSD's missions and business functions (i.e., least privilege). Accounts will be removed, and access will be denied for all those who have left the agency or moved to another department such that such access is no longer warranted.

(2) Users must comply with the administrative Password requirements.

(3) All remote connections must be made through managed points-of-entry in accordance with administrative remote access requirements.

X. **Training**

All Users of department data, data systems and data assets must annually complete the information security and privacy training offered by the MVCSD. Information security and privacy training will be made available to all Users. MVCSD Employees must complete the training at least annually.