

To accomplish MC<sup>2</sup>'s mission and comply with the law, the MC<sup>2</sup> must collect, create and store information. Accurately maintaining and protecting this data is important for efficient MC<sup>2</sup> operations, compliance with laws mandating confidentiality, and maintaining the trust of the MC<sup>2</sup>'s stakeholders. All persons who have access to MC<sup>2</sup> data are required to follow state and federal law, MC<sup>2</sup> policies and procedures, and other rules created to protect the information.

The provisions of this policy shall supersede and take precedence over any contrary provisions of any other policy adopted prior to the date of this policy.

**A. Definitions**

Confidential Data/Information - Information that the MC<sup>2</sup> is prohibited by law, policy or contract from disclosing or that the MC<sup>2</sup> may disclose only in limited circumstances. Confidential data includes, but is not limited to, personally identifiable information regarding students and employees.

Critical Data/Information - Information that is determined to be essential to MC<sup>2</sup> operations and that must be accurately and securely maintained to avoid disruption to MC<sup>2</sup> operations. Critical data is not necessarily confidential.

**B. Data and Privacy Governance Plan - Administrative Procedures.**

1. Data Governance Plan. The CEO, in consultation with the MC<sup>2</sup> Information Security Officer ("ISO") (see paragraph C, below) shall create a Data and Privacy Governance Plan ("Data Governance Plan"), to be presented to the Board no later than June 30, 2019. Thereafter, the CEO, in consultation with the ISO, shall update the Data Governance Plan for presentation to the Board no later than June 30 each year.

The Data Governance Plan shall include:

- (a) An inventory of all software applications, digital tools, and extensions. The inventory shall include users of the applications, the provider, purpose, publisher, privacy statement, and terms of use;
- (b) A review of all software applications, digital tools, and extensions and an assurance that they meet or exceed minimum standards set by the New Hampshire Department of Education;
- (c) Policies and procedures for access to data and protection of privacy for students and

staff including acceptable use policy for applications, digital tools, and extensions used on District hardware, server(s) or through the District network(s);

(d) A response plan for any breach of information; and

(e) A requirement for a service provider to meet or exceed standards for data protection and privacy.

2. Policies and Administrative Procedures. The CEO, in consultation with the ISO, is directed to review, modify and recommend (policies) create (administrative procedures), where necessary, relative to collecting, securing, and correctly disposing of MC<sup>2</sup> data (including, but not limited to Confidential and Critical Data/Information, and as otherwise necessary to implement this policy and the Data Governance Plan. Such policies and/or procedures will may or may not be included in the annual Data Governance Plan.

**C. Information Security Officer.**

The MC<sup>2</sup> Information Communications Technology Specialist is hereby designated as the MC<sup>2</sup>'s Information Security Officer (ISO) and reports directly to the CEO or designee. The ISO is responsible for implementing and enforcing MC<sup>2</sup>'s security policies and administrative procedures applicable to digital and other electronic data, and suggesting changes to these policies, the Data Governance Plan, and procedures to better protect the confidentiality and security of MC<sup>2</sup>'s data. The ISO will work with the both MC<sup>2</sup> and building level administrators and Data managers (paragraph E, below) to advocate for resources, including training, to best secure the MC<sup>2</sup>'s data.

The CFO is MC<sup>2</sup>'s alternate ISO and will assume the responsibilities of the ISO when the ISO is not available.

**D. Responsibility and Data Stewardship.**

All MC<sup>2</sup> employees, volunteers and agents are responsible for accurately collecting, maintaining and securing MC<sup>2</sup> data including, but not limited to, Confidential and/or Critical Data/Information.

**E. Data Managers.**

All MC<sup>2</sup> administrators are data managers for all data collected, maintained, used and disseminated under their supervision as well as data they have been assigned to manage in the MC<sup>2</sup>'s data inventory. Data managers will monitor employee access to the information to ensure that confidential information is accessed only by employees who need the information to provide services to the MC<sup>2</sup> and that confidential and critical information is modified only by authorized employees. Data managers will assist the ISO in enforcing MC<sup>2</sup> policies and procedures regarding data management.

**F. Confidential and Critical Information.**

MC<sup>2</sup> will collect, create or store confidential information only when the CEO or designee determines it is necessary, and in accordance with applicable law. The District will provide access to confidential information to appropriately trained MC<sup>2</sup> employees and volunteers only when the MC<sup>2</sup> determines that such access is necessary for the performance of their duties. MC<sup>2</sup> will disclose confidential information only to authorized MC<sup>2</sup> contractors or agents who need access to the information to provide services to MC<sup>2</sup> and who agree not to disclose the information to any other party except as allowed by law and authorized by MC<sup>2</sup>.

MC<sup>2</sup> employees, contractors and agents will notify the ISO or designee immediately if there is reason to believe confidential information has been disclosed to an unauthorized person or any information has been compromised, whether intentionally or otherwise. The ISO or designee will investigate immediately and take any action necessary to secure the information, issue all required legal notices and prevent future incidents. When necessary, the CEO, ISO or designee is authorized to secure resources to assist MC<sup>2</sup> in promptly and appropriately addressing a security breach.

Likewise, MC<sup>2</sup> will take steps to ensure that critical information is secure and is not inappropriately altered, deleted, destroyed or rendered inaccessible. Access to critical information will only be provided to authorized individuals in a manner that keeps the information secure.

MC<sup>2</sup> staff, volunteers, contractors and agents who are granted access to critical or confidential information/data are required to keep the information secure and are prohibited from disclosing or assisting in the unauthorized disclosure of such confidential or critical data/information. All individuals using confidential and critical data/information will strictly observe all administrative procedures, policies and other protections put into place by the District including, but not limited to, maintaining information in locked rooms or drawers, limiting access to electronic files, updating and maintaining the confidentiality of password protections, encrypting and redacting information, and disposing of information no longer needed in a confidential and secure manner.

#### **G. Using Online Services and Applications.**

MC<sup>2</sup> staff members are encouraged to research and utilize online services or applications to engage students and further the MC<sup>2</sup>'s education mission. MC<sup>2</sup> employees, however, are prohibited from installing or using applications, programs or other software, or online system/website, that either stores, collects or shares confidential or critical data/information, until the ISO approves the vendor and the software or service used. Before approving the use or purchase of any such software or online service, the ISO or designee shall verify that it meets the requirements of the law, Board policy, and the Data Governance Plan, and that it appropriately protects confidential and critical data/information. This prior approval is also required whether or not the software or online service is obtained or used without charge.

#### **H. Training.**

The ISO will provide appropriate training to employees who have access to confidential or critical information to prevent unauthorized disclosures or breaches in security. All school employees will receive annual training in the confidentiality of student records, and the requirements of this policy and related procedures and rules.

#### **I. Data Retention and Deletion.**

The ISO or designee shall establish a retention schedule for the regular archiving and deletion of data stored on MC<sup>2</sup> technology resources. The retention schedule should comply with, and be

incorporated into the data/record retention schedule established under Policy EHB and administrative procedure EHB-R, including but not limited to, provisions relating to Litigation and Right to Know holds as described in Policy EHB.

#### **J. Consequences**

Employees who fail to follow the law or MC<sup>2</sup>'s policies or procedures regarding data governance and security (including failing to report) may be disciplined, up to and including

termination. Volunteers may be excluded from providing services to MC<sup>2</sup>. MC<sup>2</sup> will end business relationships with any contractor who fails to follow the law, MC<sup>2</sup> policies or procedures, or the confidentiality provisions of any contract. In addition, MC<sup>2</sup> reserves the right to seek all other legal remedies, including criminal and civil action and seeking discipline of an employee's teaching certificate.

MC<sup>2</sup> may suspend all access to data or use of MC<sup>2</sup> technology resources pending an investigation. Violations may result in temporary, long-term or permanent suspension of user privileges. MC<sup>2</sup> will cooperate with law enforcement in investigating any unlawful actions. The CEO or designee has the authority to sign any criminal complaint on behalf of MC<sup>2</sup>.

Any attempted violation of MC<sup>2</sup>'s policies, procedures or other rules will result in the same consequences, regardless of the success of the attempt.

**Legal References:**

*15 U.S.C. §§ 6501-6506 \* Children's Online Privacy Protection Act (COPPA)*

*20 U.S.C. § 1232g \* Family Educational Rights and Privacy Act (FERPA)*

*20 U.S.C. § 1232h \* Protection of Pupil Rights Amendment (PPRA)*

*20 U.S.C. § 1400-1417 \* Individuals with Disabilities Education Act (IDEA)*

*20 U.S.C. § 7926 \* Elementary and Secondary Education Act (ESSA)*

*RSA 189:65 \* Definitions*

*RSA 186:66 \* Student Information Protection and Privacy*

*RSA 189:67 \* Limits on Disclosure of Information*

*RSA 189:68 \* Student Privacy*

*RSA 189:68-a \* Student Online Personal Information*

*RSA 359-C:19-21 \* Right to Privacy/Notice of Security Breach*

Appendix Reference:

Date Adopted: May 20, 2019

Revision Dates:

Last Review Date: