DATA GOVERNANCE AND SECURITY

Category: Priority Required by Law ***Related Policies: DFGA, EHAA, EHAC, EHB, GBEBD, IHBH, JICJ, JICL, KD, & KDC***

To accomplish the Mascoma Valley Regional School District's mission and comply with the law, the District must collect, create and store information. Accurately maintaining and protecting this data is important for efficient District operations, compliance with laws mandating confidentiality, and maintaining the trust of the District's stakeholders. All persons who have access to District data are required to follow state and federal law, District 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 District is prohibited by law, policy, or contract from disclosing or that the District may disclose only in limited circumstances. Confidential data includes, but is not limited to, personally identifiable information (i.e., "PII") regarding students and employees.

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

Cybersecurity Incident – an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information processes, stores, or transmits, if that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

B. Data and Privacy Governance Plan - Administrative Procedures.

1. Data Governance Plan. The Superintendent, in consultation with the District Information Security Officer ("ISO") (see paragraph C, below), shall update the Data and Privacy Governance Plan ("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/cybersecurity incidents; see RSA 31:103-b and RSA 359-C:19-21;

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

f. A provision that students participating in career exploration or career technical education may, **with written parental consent**, register for technology platforms and services to be used as part of the student's approved program of study, which require the provision of personally identifiable information. Copies of written parental consent shall be retained as part of a student's educational record.

The Data Governance Plan shall include standards and provisions that meet or exceed the standards set forth in the N.H. Dept. of Education's *Minimum Standards for Privacy and Security of Student and Employee Data.*

2. Policies and Administrative Procedures. The Superintendent, 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 District 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 may or may not be included in the annual Data Governance Plan.

C. Information Security Officer.

The Director of Technology is hereby designated as the District's Information Security Officer (ISO) and reports directly to the Superintendent or designee. The ISO is responsible for implementing and enforcing the District'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 District data. The ISO will work with both the District and building level administrators and Data managers (paragraph E, below) to advocate for resources, including training, to best secure the District's data.

The Business Administrator is the District's alternate ISO and will assume the responsibilities of the ISO when the ISO is not available.

D. Responsibility and Data Stewardship.

All District employees, volunteers and agents are responsible for accurately collecting, maintaining, and securing District data including, but not limited to, confidential and/or critical data/information.

E. Data Managers.

All District 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 District'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 District and that confidential and critical information is modified only by authorized employees. Data managers will assist the ISO in enforcing District policies and procedures regarding data management.

F. Confidential and Critical Information.

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

District 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 Superintendent and/or the ISO shall immediately report any known or suspected cybersecurity incidents within the District's information systems, or within an information system of any vendor of the District, to the New Hampshire Cyber Integration Center of the Department of Information Technology. The Superintendent and/or the ISO shall disclose all known information and interactions. See RSA 31:103-b.

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 Superintendent, ISO, or designee is authorized to secure resources to assist the District in promptly and appropriately addressing a security breach.

As a part of this investigation, the ISO or designee will promptly determine the likelihood that any information part of a cybersecurity incident has been or will be misused. If the determination is that the misuse of information has occurred or is reasonably likely to occur, or if a determination cannot be made, the ISO will notify the affected individuals as soon as possible, consistent with the notification requirements under RSA 359-C:20.

Likewise, the District 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.

All District 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.

District staff members are encouraged to research and utilize online services or applications to engage students and further the District's education mission. District 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.

Notwithstanding the prohibition on the use of applications, etc. that store, collect or share personally identifiable information concerning a student ("PII"), students participating in career exploration or career technical education may, **with written parental consent**, register for technology platforms and services to be used as part of the student's approved program of study, even if said platforms and services require the collection, storage and sharing of the student's PII. Use of these platforms and services is subject to the conditions set forth in B.1(f), above, and related provisions of the Data Governance Plan. The written parental consent forms shall be retained as student records.

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 District technology resources. The retention schedule should comply with, and be incorporated into the data/record retention schedule established under Board policy EHB and administrative procedure EHB-R], including but not limited to, provisions relating to Litigation and Right to Know holds as described in Board policy EHB].

J. Consequences

Employees who fail to follow the law, or District 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 the District. The District will end business relationships with any contractor who fails to follow the law, District policies or procedures, or the confidentiality provisions of any contract. In addition, the District reserves the right to seek all other legal remedies, including criminal and civil action and seeking discipline of an employee's teaching certificate.

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

Any attempted violation of District policies, procedures, or other rules will result in the same consequences, regardless of the success of the attempt.

***Legal References Disclaimer**: These references are not intended to be considered part of this policy, nor should they be taken as a comprehensive statement of the legal basis for the Board to enact this policy, nor as a complete recitation of related legal authority. Instead, they are provided as additional resources for those interested in the subject matter of the policy.*

NH Statutes	**Description**
RSA 189:65	Definitions
RSA 189:66	Data Inventory and Policies Publication
RSA 189:67	Limits on Disclosure of Information
RSA 189:68	Student Privacy
RSA 189:68-a	Student Online Personal Information
RSA 31:103-b	Cybersecurity
RSA 359-C:19-21	Right to Privacy/Notice of Security Breach

Federal Statutes	**Description**
15 U.S.C. §§ 6501-6506	Children's Online Privacy Protection Act (COPPA)
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)
20 U.S.C. §1232g	Family Educational Rights and Privacy Act (FERPA)

Reviewed by EIC: 6/20/19; 1st Reading: 6/22/19; 2nd Reading/Adopted: 7/23/19
Reviewed/1st Reading: 10/25/22; 2nd Reading/Adopted: 11/8/22
Reviewed/1st Reading: 11/28/23, 12/12/23; 2nd Reading/Adopted: 1/9/24