Monadnock Regional School District & SAU #93
School Board Agenda
June 6, 2023

In-Person MRMHS Library & Webinar Link 7:00 pm

Join Zoom Meeting:
https://mrsd-org.zoom.us/j/84904072167?pwd=dWRXdnNGbmkrUDFrRGpsYjlyUGtCQT09

ID: 84904072167 Passcode: 007496 (US) +1 312-626-6799 **Passcode: 007496**

The public is encouraged to attend MRSD Board meetings.
Comments are welcome during the 'Public Comments' portions of the agenda.

"We collaborate not just to teach, but also to engage and educate every student in our district in an environment that is challenging, caring, and safe, while fostering lifelong learning."

1. CALL THE MEETING TO ORDER 7:00 pm
2. PUBLIC COMMENTS (15 minutes)
3. #celebrateMRSD
    - a. * Track & Field State Champion Jacket
4. MATTERS FOR SCHOOL BOARD INFORMATION & DISCUSSION
    - a. 2024/25 Budget Proposals
    - b. NHSBA Call for Resolutions
    - c. Board Member Stipends
5. MATTERS THAT REQUIRE BOARD ACTION
    - a. * Annual Approval of Data Governance Plan (online packet only)
    - b. * May 16, 2023 Joint School Board & Budget Minutes
    - c. * Charter & Goals: Finance/Facilities
    - a. * SOW for Superintendent Search
    - d. * Principal Search Committee - Timeline and Composition
    - e. * Diligent Modern Governance Seminar
    - f. * Manifest
    - g. * Authorize School Board Members to Sign Summer Manifests
    - h. * Budget Transfers
    - i. * Authorize Superintendent to hire certified staff through 9/5/2023
6. SETTING NEXT MEETING'S AGENDA
7. PUBLIC COMMENTS (15 minutes)
8. NON-PUBLIC SESSIONS under RSA 91-A:3. II
    - a. (a) The dismissal, promotion, or compensation of any public employee
        - i. Approve non-affiliated salaries and wages
        - ii. Notification of non-certified staff renewals
    - b. Other non-public sessions as needed
9. ADJOURNMENT

**Indicates an item requiring action. The order of the agenda is subject to change.*

SINGLE DISTRICT SCHOOL ADMINISTRATIVE UNITS

RSA 94-C:3 – Single District School Administrative Units; Exemption. Single district school administrative units shall be considered the same as a single school district and shall be exempt from meeting the requirements of this chapter, except that they shall provide superintendent services pursuant to RSA 194-C:4

NONPUBLIC SESSIONS

RSA 91-A:3– II. Only the following matters shall be considered or acted upon in nonpublic session:

(a) **The dismissal, promotion, or compensation of any public employee** or the disciplining of such employee, or the investigation of any charges against him or her, unless the employee affected (1) has a right to a meeting and (2) requests that the meeting be open, in which case the request shall be granted.

(b) The **hiring** of any person as a public employee.

(c) Matters which, if discussed in public, would likely adversely affect the **reputation** of any person, other than a member of the public body itself, unless such person requests an open meeting.

(d) Consideration of the **acquisition, sale, or lease of real or personal property** which, if discussed in public, would likely benefit a party or parties whose interests are adverse to those of the general community.

(e) **Consideration or negotiation of pending claims or litigation** which has been threatened in writing or filed by or against the public body or any subdivision thereof, or by or against any member thereof because of his or her membership in such public body, until the claim or litigation has been fully adjudicated or otherwise settled.

(i) Consideration of matters relating to the **preparation for and the carrying out of emergency functions**, including training to carry out such functions, developed by local or state safety officials that are directly intended to thwart a deliberate act that is intended to result in widespread or severe damage to property or widespread injury or loss of life.

(j) **Consideration of confidential, commercial, or financial information** that is exempt from public disclosure under RSA 91-A:5, IV in an adjudicative proceeding pursuant to RSA 541 or RSA 541-A.

(k) Consideration by a school board of entering into a **student or pupil tuition contrac**t authorized by RSA 194 or RSA 195-A,

(l) **Consideration of legal advice provided by legal counsel**, either in writing or orally, to one or more members of the public body, even where legal counsel is not present.

CALENDAR OF UPCOMING MRSD MEETINGS:

6/8/2023	**Extra-Curricular Committee**	**6:00 pm**	**SAU Conference Room**
6/13/2023	**Finance & Facilities Committee**	**7:00 pm**	**SAU Conference Room**
6/20/2023	**MRSD/SAU 93 School Board**	**7:00 pm**	**MRMHS Library**
6/22/2023	**Extra-Curricular Committee**	**6:00 pm**	**SAU Conference Room**
6/27/2023	**Budget Committee**	**7:00 pm**	**MRMHS Library**
6/27/2023	**Policy Committee**	**7:00 pm**	**SAU Conference Room**

Meetings will be in person for all Board & Committee Members. The public is encouraged & welcome to attend either in person or through Zoom. Public comments are welcome in person during the 'Public Comments' portions of the agenda.

**** Please note: All Committee Meetings dates, times, and locations are posted in the SAU 93 Reception Lobby, on the MRSD website calendar, and in the schools and towns of MRSD. In the event of a snow day, the school board meeting will be planned for the following school day.****

Monadnock Regional School District

Data Governance Plan

Contents

Introduction

The Monadnock Regional School District is committed to protecting our students' and staffs' privacy through maintaining strong privacy and security protections. The privacy and security of this information is a significant responsibility, and we value the trust of our students, parents, and staff.

The Monadnock Regional School District's Data Governance Plan includes information regarding the data governance team, data and information governance, applicable School Board policies, District procedures, as well as applicable appendices and referenced supplemental resources.

This manual outlines how operational and instructional activity shall be carried out to ensure the District's data is accurate, accessible, consistent, and protected. The document establishes who is responsible for information under various circumstances and specifies what procedures shall be used to manage and protect it. Definitions of terminology can be found in Appendix A: Definitions.

The Monadnock Regional School District's Data Governance Plan shall be a living document. To make the document flexible, details are outlined in the appendices and referenced supplemental resources. This document and any future modifications to this document will be posted on the District's website.

Data Governance Team

The Monadnock Regional School District's Data Governance team consists of the following positions: Superintendent, Curriculum Director, Business Administrator, Facilities Director, Human Resources Manager, Director of Special Services and the Director of Technology. Members of the Data Governance Team will act as data stewards for all data under their direction. The Director of Technology will act as the Information Security Officer (ISO), with assistance from members of the full Technology team. The Business Administrator is the district's alternate ISO and will assume the responsibilities of the ISO when the ISO is not available. All members of the district administrative team will serve in an advisory capacity as needed.

Purpose

The School Board recognizes the value and importance of a wide range of technologies for a well-rounded education, enhancing the educational opportunities and achievement of students. The Monadnock Regional School District provides its faculty, staff, and administrative staff access to technology devices, software systems, network and Internet services to support research and education. All components of technology must be used in ways that are legal, respectful of the rights of others, and protective of juveniles and that promote the educational objectives of Monadnock Regional School District.

To that end, the district must collect, create and store confidential information. Accurately maintaining and protecting this data is important for efficient district operations, compliance with laws mandating confidentiality, and maintaining the trust of all district 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.

It is the policy of the Monadnock Regional School District that data or information in all its forms, written, electronic, or printed, is protected from accidental or intentional unauthorized modification, destruction or disclosure throughout its life cycle. This protection includes an appropriate level of security over the equipment, software, and practices used to process, store, and transmit data or information. All staff and authorized district contractors or agents using confidential information will strictly observe protections put into place by the district.

Scope

The data security policy, standards, processes, and procedures apply to all students and staff of the district, contractual third parties and agents of the district, and volunteers who have access to district data systems or data. This policy applies to all forms of Monadnock Regional School District data and information, including but not limited to:

- Speech, spoken face to face, or communicated by phone or any current and future technologies.
- Hard copy data printed or written.
- Communications sent by post/courier, fax, electronic mail, text, chat and/or any form of social media.
- Data stored and/or processed by any electronic device, including servers, computers, tablets, mobile devices.
- Data stored on any type of internal, external, or removable media or cloud based services.
- The terms data and information are used separately, together, and interchangeably throughout the policy, the intent is the same.
- Any computer, laptop, mobile device, printing and/or scanning device, network appliance/equipment, AV equipment, server, internal or external storage, communication device or any other current or future electronic or technological device may be referred to as systems, assets or resources.
- All involved systems and information are considered assets of the Monadnock Regional School District and shall be protected from misuse, unauthorized manipulation, and destruction.

Regulatory Compliance

The district will abide by any law, statutory, regulatory, or contractual obligations affecting its data systems (see Appendix B: Laws, Statutory, and Regulatory Security Requirements). The Monadnock Regional School District complies with or exceeds the NH Minimum Standards for Privacy and Security of Student and Employee Data, and standards applicable to data governance are addressed throughout this Data Governance Plan. The Monadnock Regional School District complies with all other applicable regulatory acts including but not limited to the following:

- Children's Internet Protection Act (CIPA)
- Children's Online Privacy Protection Act (COPPA)
- Family Educational Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Payment Card Industry Data Security Standard (PCI DSS)
- Protection of Pupil Rights Amendment (PPRA)
- Individuals with Disabilities in Education Act (IDEA)
- New Hampshire State RSA - Student and Teacher Information Protection and Privacy

    NH RSA 189:65 Definitions

    NH RSA 189:66 Data Inventory and Policies Publication

    NH RSA 189:67 Limits on Disclosure of Information

    NH 189:68 Student Privacy

    NH RSA 189:68-a - Student Online Personal Information
- NH Minimum Standards for Privacy and Security of Student and Employee Data (see Appendix O)
- New Hampshire State RSA - Right to Privacy:

NH RSA 359-C:19 - Notice of Security Breach Definitions

NH RSA 359-C:20 - Notice of Security Breach Required

NH RSA 359-C:21 - Notice of Security Breach Violation

Data User Compliance

The Data Governance Plan applies to all users of Monadnock Regional School District’s information including: staff, students, volunteers, and authorized district contractors or agents. All data users are to maintain compliance with School Board Policies and District administrative procedures JICL/GBEF (Employee and Student Acceptable Computer & Intranet/Internet Use), JICL-R (Information Technology Responsible Use Policy Form) and all policies, procedures, and resources as outlined within this Data Governance Plan and School Board Policy.

A consistently high level of personal responsibility is expected of all users granted access to the district’s technology resources. Any violation of district policies or procedures regarding technology usage may result in temporary, long-term or permanent suspension of user privileges. User privileges may be suspended pending investigation into the use of the district’s technology resources.

Unless permission has been granted by the ISO or designee, no staff, vendor or other person may remove confidential or critical data from the district's premises or the district's network, remove a device containing confidential or critical data from the district's premises, or modify or copy confidential or critical data for use outside the district. If permission is given, the data may be accessed only on a district-provided device with appropriate security controls or through a secure virtual private network (VPN). When users access confidential or critical data from a remote location, the user must take precautions to ensure that the confidential or critical data is not downloaded, copied or otherwise used in a manner that would compromise the security and confidentiality of the information.

Staff who fail to follow the law or district policies or procedures regarding data governance and security may be disciplined or terminated. 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 a staff member’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.

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

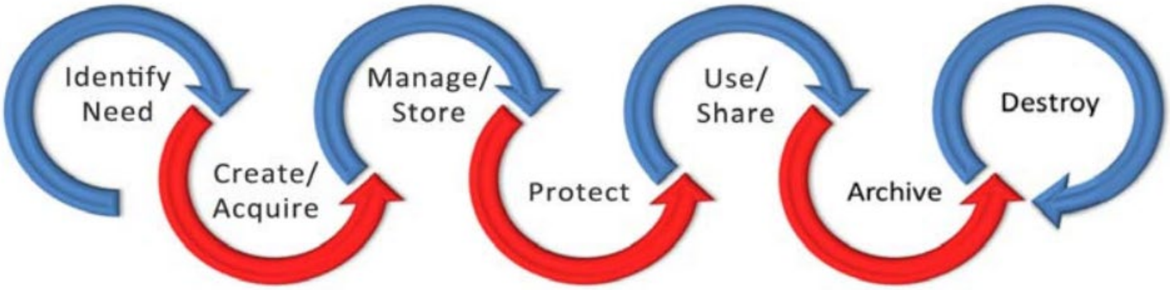
- Unauthorized disclosure of PII or Confidential Information.
- Sharing your user IDs or passwords with others (exception for authorized technology staff for the purpose of support)
- Applying for a user ID under false pretenses or using another person’s ID or password.
- Unauthorized use of an authorized password to invade student or staff privacy by examining records or information for which there has been no request for review.
- The unauthorized copying of system files.
- Attempting to secure a higher level of privilege without authorization.
- Installation or use of unlicensed software or software not approved for district technological

systems.

- The intentional unauthorized altering, destruction, or disposal of district information, data and/or systems. This includes the unauthorized removal of technological systems such as but not limited to: laptops, internal or external storage, computers, servers, backups or other media, that may contain PII or confidential information.
- The introduction of computer viruses, hacking tools or other disruptive or destructive programs.

Data Lifecycle

Data Governance is necessary at each phase in the data lifecycle. This lifecycle starts at evaluating the need for data collection and ends when the data is destroyed. It is important that appropriate safeguards, policies, procedures and practices are in place for each phase of the data lifecycle.



Identifying Need & Assessing Systems for District Requirements

To accomplish the district's mission and to comply with the law, the district may need to maintain confidential information, including information regarding students, parents/guardians, staff, applicants for employment and others. The district will collect, create or store confidential information only when the Superintendent or designee determines it is necessary.

New Systems

District staff members are encouraged to research and utilize online services or applications to engage students and further the district's educational mission. However, before any online service or application is purchased or used to collect or store confidential or critical information, including confidential information regarding students or staff, the ISO or designee must approve the use of the service or application and verify that it meets the requirements of the law and School Board policy and appropriately protects confidential and critical information. This prior approval is also required when the services are obtained without charge.

The Monadnock Regional School District will establish a process for vetting new digital resources to ensure that all new resources meet business and/or instructional need as well as security requirements.

Memorandums of understanding (MOU), contracts, terms of use and privacy policy for any system that creates, collects or uses personally identifiable information (PII), student records or confidential data must be reviewed by the ISO prior to initiation.

All new resources shall be properly evaluated against the following criteria, when applicable:

- Impact on technology environment including storage and bandwidth
- Hardware requirements, including any additional hardware
- License requirements/structure, number of licenses needed, and renewal cost
- Maintenance agreements including cost
- Resource update and maintenance schedule

- Funding for the initial purchase and continued licenses and maintenance
- Evaluate terms of service, privacy policy, and MOU/contract that meet the following criteria:

  o The district continues to own the data shared, and all data must be available to the district upon request.

  o The vendor's access to and use of district data is limited; the data cannot be used for marketing, targeted advertising or data mining; and the data cannot be shared with third parties unless allowed by law and authorized by the district. If metadata is collected, it will be protected to the same extent as the district's confidential or critical information.

  o District data will be maintained in a secure manner by applying appropriate technical, physical and administrative safeguards to protect the data.

  o The provider will comply with district guidelines for data transfer or destruction when contractual agreement is terminated.

  o No API will be implemented without full consent of the district.

  o All data will be treated in accordance to federal, state and local regulations

  o The provider assumes liability and provides appropriate notification in the event of a data breach.

  Note: Exceptions can be made by the ISO when all the criteria cannot be met for a legitimate reason while still meeting all regulatory requirements for use. Parent permission is requested from parents during the yearly online registration process for district vetted and approved applications and tools.

Review of Existing Systems

The District will ensure that data collection is aligned with School Board Policy EHAB. Data systems shall be regularly reviewed to ensure that only necessary data is being transmitted and collected.

Individual student level data is submitted to different approved service providers in order to ensure business operations and instructional services. At times, these imports include PII for staff and students. The District must ensure that each piece of PII is necessary for operations or instruction and that the providers are abiding by their terms of service.

The District will audit data imports annually. These audits should include:

- Review of provider’s terms of service to ensure they meet the District’s data security requirements.
- Verification that software imports are accurate and pulling the correct information.
- Verification that, when applicable, the staff, students and classes included in the imports are still necessary for instructional purposes (only those that need data collected are included in import).
- Determine if the fields included in the imports are still necessary for intended purpose.

Acquisition and Creation

After completing the requirements for adoption of any new systems, staff shall complete an online request form for any new digital app/tool that either has an associated cost or collects staff or student data (see Appendix C: Digital Resource Acquisition and Use). All staff must adhere to the following guidelines regarding a new digital resource acquisition:

- Contracts for any system that creates, collects or uses personally identifiable information (PII), student records or confidential data must be reviewed by the ISO prior to initiation. Staff should speak with their building Principal before using ANY new app/online tool with students and seek their assistance with the evaluation/vetting process. This includes any online tool that a student interacts with where they may be creating content and/or any site that requires any student login.

- It is the responsibility of the staff requesting to use new digital content to properly vet the resource to ensure that it meets district business objectives, is in line with curriculum or behavioral standards, is age appropriate, is instructionally sound, and is appropriate for the intended use.
- Digital resources that accompany adopted instructional and/or curriculum materials will be vetted by the Curriculum Director and the ISO, or designee, prior to purchase.

Management and Storage

Systems Security

The district will provide access to confidential information to appropriately trained district staff 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 (School Board Policy EHAB). Therefore, systems access will only be given on an as-needed basis as determined by the data manager and ISO. Further information regarding Electronic Access Security Controls is contained in the Security/Protection section of this manual.

Data Management

The effective education of students and management of district personnel often require the district to collect information, some of which is considered confidential by law and district policy. In addition, the district maintains information that is critical to district operations and that must be accurately and securely maintained to avoid disruption to district operations.

Data Managers are responsible for the development and execution of practices and procedures that ensure the accuracy and security of data in an effective manner. 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. Data managers will:

- ensure that system account creation procedures and data access guidelines appropriately match staff member job function with the data on instructional and operational systems.
- review all staff with custom data access beyond their typical group’s access.
- review district processes to ensure that data will be tracked accurately.
- review contracts with instructional and operational software providers to ensure that they are current and meet the district data security guidelines.
- ensure that staff are trained in the district’s proper procedures and practices in order to ensure accuracy and security of data.
- assist the ISO in enforcing district policies and procedures regarding data management.

Security/Protection

Risk Management

A thorough risk analysis of all Monadnock Regional School District’s data networks, systems, policies, and procedures shall be conducted on an annual or biennial basis by an external third party or as requested by the Superintendent, ISO or designee. An internal audit of District network security will be conducted annually by District Technology staff. This analysis shall be completed using the risk management steps outlined in the Data Security Checklist (see Appendix D: Data Security Checklist). The product of the risk analysis will be referred to as the risk assessment. The risk assessment shall be used to develop a plan to mitigate identified threats and risk to an acceptable level by reducing the extent of vulnerabilities.

Security Logs

The District will maintain a comprehensive list of critical system events that will be logged and monitored to ensure data security. These events will include, but are not limited to, access to critical systems and modification of critical data. When applicable, notifications will be established for critical event triggers.

Physical Security Controls

Technology telecommunication closets are housed in secure locations. Access authorization is assigned through the Director of Technology, Network Administrator and or Director of Facilities. In addition, access to areas in which information processing is carried out shall be restricted to only appropriately authorized individuals (see Appendix G: Physical Security Controls).

No technological systems shall be disposed of or moved without adhering to the appropriate procedures (see Appendix H: Asset Management).

Inventory Management

The district shall maintain a process for inventory control in accordance to federal and state requirements and School Board policy. All district technology assets will be maintained in inventory and verified through the regular inventory verification process (see Appendix H: Asset Management).

Virus, Malware, Spyware, Phishing and SPAM Protection

The District uses a multi-layered approach to ensure that all electronic files are appropriately scanned for viruses, malware, spyware, phishing and SPAM. These include, but are not limited to, enterprise virus / malware / spyware software, group policy, gateways, firewalls, and content filters. Users shall not turn off or disable district protection systems or install other systems (see Appendix I: Virus, Malware, Spyware, Phishing and SPAM Protection).

Electronic Access Security Controls

District staff will only access personally identifiable and/or confidential information if necessary to perform their duties. The district will only disclose this information 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.

Mechanisms to control access to PII, confidential information, internal information and computing resources include, but are not limited to, the following methods:

- **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 will be held accountable for all actions performed on the system with their User ID. User accounts and passwords shall not be shared.
- **Authorization:** Access controls are maintained through a partnership between the technology department, human resources (HR) and data managers.

Additionally, only members of the District Technology staff will be granted access to domain level administrator and local machine administrator accounts in order to complete their job functions.

Access security is audited annually or whenever access permission requirements are changed for a particular application/software or when an application/software is no longer necessary.

Staff Users

All new staff accounts are authorized through an HR hiring process (see Appendix J: Account Management). Role-based permissions and security groups are used to establish access to all systems (see Appendix K: Data Access Roles and Permissions). If a staff member requires additional access, a request must be made directly to the ISO with a clear justification for access.

Contractors/Vendors

Access to contractors/vendors is governed through the same process using School Board Policy EHAB. All contractor/vendor access must be approved by HR and the ISO. All contractors doing business on district premises must also pass a background check unless other security measures are addressed in a vendor contract. All contractors/vendors accessing district data will be considered on premise users. Once the approval has been obtained, the technology department will create the account, only granting access to the server/application that the contractor/vendor supports.

Password Security

The District will enforce secure passwords for all systems within their control (see Appendix L: Password Security). When possible, the district will utilize Single Sign On (SSO) or LDAP/Active Directory Integration to maintain optimal account security controls.

Concurrent Sessions

When possible, the district will limit the number of concurrent sessions for a user account in a system.

Remote Access

Access into the District's network from outside is strictly prohibited without explicit authorization from the ISO. Remote access will be granted through virtual private network (VPN) connection through the district's network VPN appliance; no other method of remote access shall be granted without explicit authorization from the ISO. PII, confidential information and/or Internal Information that is stored or accessed remotely shall maintain the same level of protection as information stored and accessed within District's network.

In the event that VPN access is needed by a contractor/vendor, access must be approved by the ISO. The Network Administrator will establish the contractor account, only granting access to the server/application that the contractor/vendor supports.

All VPN accounts will be reviewed at least annually.

Securing Data at Rest and Transit

District data security applies to all forms of data, including data stored on devices, data in transit and data stored on additional resources. All district external hard drives will be maintained in inventory and verified through the regular inventory verification process. Regular transmission of student data to internal and external services is managed by the technology department using a secure data transfer protocol.

Users must ensure that they are securely storing their data. Guidelines have been established for Cloud Storage and File Sharing, External Storage Devices, and File Transmission Practices. (see Appendix F: Securing Data at Rest and Transit). These guidelines are outlined in the following section.

Usage and Dissemination

A consistently high level of personal responsibility is expected of all users granted access to the district's technology resources. All district staff, volunteers, contractors and agents who are granted access to critical and confidential information are required to keep the information secure and are prohibited from disclosing or assisting in the unauthorized disclosure of confidential information. All individuals using confidential and critical information will strictly observe 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 in a confidential and secure manner.

All users are responsible for the security and integrity of the data they create, store or access. Users are expected to act as good stewards of data and treat data security and integrity with a high degree of responsibility and priority. Users must follow all guidelines outlined with Board policies, specifically Employee and Student Technology Usage (JICL/GBEF, JICL-R), and Student Records (JRA, JRA-R).

District staff, 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.

Data Storage and Transmission

All staff and students that log into district owned computers will be provided with several options for data storage and transmission. Staff and students will need to ensure that they are securely storing their data. Staff and students will be able to store data on the local device. It is important to note that this data is not a part of the district's continuity plan, and thus will not be backed up by the district's backup solution. Staff will also have a mapped personal folder. This folder acts as a redirection of document and desktop folders to district file servers. Access to these files is restricted to the folder's owner (staff who is assigned) and district enterprise administrator accounts. Staff and students using Chromebook devices have limited local storage capabilities. Chromebook users are to store data within their G Suite for Education Drive account.

Cloud Storage and File Sharing

The term "Cloud Storage" is used to define all types of remote server storages accessed by users through the internet. All staff and students are provided with a Google G Suite for Education account that provides unlimited storage. Users are responsible for all digital content on their district provided Google G Suite for Education Drive (see Appendix F: Securing Data at Rest and Transit).

File Transmission Practices

Staff are responsible for securing sensitive data for transmission through email or other channels. Staff should not transmit files labeled classified, confidential, or restricted through email or third party file transfer services without district approval. When possible, staff should de-identify or redact any PII or confidential information prior to transmission. Regular transmission of student data to services such as a single sign on provider is managed by the technology department using a secure data transfer protocol (see Appendix F: Securing Data at Rest and Transit).

Credit Card and Electronic Payment

Users of systems that process electronic payments, including but not limited to processing credit card information, must adhere to strict guidelines regarding the protection of payment information and cardholder data. These users are responsible for adhering to the appropriate level of PCI compliance when handling such data (see Appendix F: Securing Data at Rest and Transit).

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 reviewed and approved by the Superintendent or designee. All other mass downloads of information shall be approved by the ISO and include only the minimum amount of information necessary to fulfill the request.

Printing

When possible, staff should de-identify or redact any PII or confidential information prior to printing. PII and confidential information shall not be downloaded, copied or printed indiscriminately or left unattended and open to compromise.

Oral Communications

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. 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 public areas.

Training

The district shall create and maintain a data security training program. This program will consist of the following:

- Training for all staff on technology policies and procedures, including confidentiality and data privacy.
- Additional training for new instructional staff on federal regulations and the use of digital resources and student electronic records.
- Training for all instructional staff on federal regulations and the use of digital resources and student electronic records.
- Training for district administration on federal regulations, data privacy and security.
- All training or professional learning that includes the use of data systems shall include data security.

Archival and Destruction

Once data is no longer needed, the ISO or designee will work with the data managers to ensure that it is appropriately destroyed. Special care will be taken to ensure that confidential information is destroyed appropriately and in accordance with law. Confidential paper records will be destroyed using methods that render them unreadable, such as shredding. Confidential digital records will be destroyed using methods that render the record irretrievable.

District Data Destruction Processes

The district will regularly review all existing data stored on district provided storage for the purposes of ensuring data identification and appropriate destruction. Data destruction processes will align with School Board Policy EHB and EHB-R. District data managers will regularly review systems and data to ensure that data that is no longer needed is destroyed. The following exceptions will be made:

- Data in an active litigation hold will be maintained until the conclusion of the hold.
- Student G Suite for Education account will be deleted after the student’s final date of attendance.
- Staff G Suite for Education accounts will be suspended after the final work day, unless HR or the ISO approves a district administrator to maintain access. Accounts will be deleted after they are no longer deemed necessary.

Asset Disposal

The district will maintain a process for physical asset disposal in accordance with School Board Policy DN. The district will ensure that all assets containing PII, confidential, or internal information are disposed of in a manner that ensures that this information is destroyed (see Appendix H: Asset Management).

Critical Incident Response

Controls shall ensure that the District can recover from any damage to or breach of 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 ISO or designee for response to a system emergency or other occurrence (for example, fire, vandalism, system failure, data breach and natural disaster) that damages/breaches data or systems.

Business Continuity

The District's administrative procedure EHB-R, delineates the timeline for data retention for all district data. The District will maintain systems that provide near-line and off-site data backup. These systems shall allow for the full recovery of critical systems in the event of a disaster. The district will test near-line and off-site backups of critical systems annually.

Disaster Recovery

The District's Technology Disaster Recovery Plan outlines critical staff, responsibilities, and processes in the event of a disaster or critical data loss. The District shall maintain a list of all critical systems and data, including contact information. The Technology Disaster Recovery Plan shall include processes that enable the District to continue operations and efficiently restore any loss of data in the event of fire, vandalism, natural disaster, or critical system failure (see Appendix M: Disaster Recovery Plan).

Data Breach Response

New Hampshire's data breach law (RSA 359-c:19, 20, 21) is triggered when a School District computer system is breached and personal information is acquired without authorization in a way that compromises the security or confidentiality of the information. The law requires a school district experiencing a breach to conduct a good faith and reasonably prompt investigation to determine the likelihood that personal information was, or will be, misused. The Data Breach Response Plan enables the District to respond effectively and efficiently to a data breach involving personally identifiable information (PII) as defined by NH Law, confidential or protected information (i.e.-FERPA), district identifiable information and other significant cybersecurity incident. The Data Breach Response Plan shall include processes to validate and contain the security breach, analyze the breach to determine scope and composition, minimize impact to the users, and provide notification (see Appendix N: Data Breach Response Plan).

Appendix A - Definitions

Confidentiality: Data or information is not made available or disclosed to unauthorized persons.

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 (PII) regarding students and staff.

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.

Data: Facts or information. Data can be in any form; oral, written, or electronic.

Data Breach, Breach of Security or Breach: A security incident in which there was unauthorized access to and unauthorized acquisition of personal information maintained in computerized form that compromises the security, confidentiality or integrity of the information.

Data Integrity: Data is current, accurate and has not been altered or destroyed in an unauthorized manner.

Data Management: The development and execution of policies, practices, and procedures in order to manage the accuracy and security of district instructional and operational data in an effective manner.

Data Owner: User responsible for the creation of data. The owner may be the primary user of that information or the person responsible for the accurate collection/recording of data. Ownership does not signify proprietary interest, and ownership may be shared. The owner of information has the responsibility for:

- knowing the information for which she/he is responsible.
- determining a data retention period for the information according to Board policy and state statute.
- ensuring appropriate procedures are in effect to protect the integrity, confidentiality, and availability of the data used or created.
- reporting promptly to the ISO the loss or misuse of data.
- initiating and/or implementing corrective actions when problems are identified.
- following existing approval processes for the selection, budgeting, purchase, and implementation of any digital resource.

Information Security Officer: The Information Security Officer (ISO) is responsible for working with the Superintendent, Data Governance Team, data managers, data owners, and users to develop and implement prudent security policies, procedures, and controls. The ISO will oversee all security audits and will act as an advisor to:

- data owners for the purpose of identification and classification of technology and data related resources.
- systems development and application owners in the implementation of security controls for information on systems, from the point of system design through testing and production implementation.

Systems: Any computer, laptop, mobile device, printing and/or scanning device, network appliance/equipment, AV equipment, server, internal or external storage, communication device or any other current or future electronic or technological device, whether hosted by the district or provider.

Security Incident: An event that 1) actually or potentially jeopardizes the confidentiality, integrity or availability of an information system or the information the system processes, stores or transmits, or 2) constitutes a violation or imminent threat of violation of security policies, security procedures or acceptable-use policies.

Personally Identifiable Information (PII): Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual‘s identity, such as name, social security number, State Assigned Student Identification, date and place of birth, mother‘s maiden name, or biometric records and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Risk: The probability of a loss of confidentiality, integrity, or availability of information resources.

User: The user is any person who has been authorized to read, enter, print or update information. A user of data is expected to:

- access information only in support of their authorized job responsibilities.
- comply with all data security procedures and guidelines.
- keep personal authentication confidential (user IDs, passwords, secure cards, PINs, access codes).
- report promptly to the ISO the loss or misuse of data.
- follow corrective actions when problems are identified.

Appendix B - Laws, Statutory, and Regulatory Security Requirements

CIPA: The Children's Internet Protection Act was enacted by Congress to address concerns about children's access to obscene or harmful content over the Internet. CIPA imposes certain requirements on schools or libraries that receive discounts for Internet access or internal connections through the E-rate program. Schools subject to CIPA have two additional certification requirements: 1) their Internet safety policies shall include monitoring the online activities of minors; and 2) as required by the Protecting Children in the 21st Century Act, they shall provide for educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyberbullying awareness and response. https://www.fcc.gov/consumers/guides/childrens-internet-protection-act

COPPA: The Children's Online Privacy Protection Act regulates operators of commercial websites or online services directed to children under 13 that collect or store information about children. Parental permission is required to gather certain information. https://www.ftc.gov/tips-advice/business-center/privacy-and-security/children%27s-privacy

FERPA: The Family Educational Rights and Privacy Act applies to all institutions that are recipients of federal aid administered by the Secretary of Education. This regulation protects student information and accords students specific rights with respect to their data.
http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

HIPAA: The Health Insurance Portability and Accountability Act applies to organizations that transmit or store Protected Health Information (PII). It is a broad standard that was originally intended to combat waste, fraud, and abuse in health care delivery and health insurance, but is now used to measure and improve the security of health information as well.
https://www.hhs.gov/hipaa/index.html

IDEA: The Individuals with Disabilities in Education Act (IDEA) is a law that makes available a free appropriate public education to eligible children with disabilities throughout the nation and ensures special education and related services to those children.
https://sites.ed.gov/idea/

PCI DSS: The Payment Card Industry Data Security Standard was created by a consortium of payment brands including American Express, Discover, MasterCard, and Visa. It covers the management of payment card data and is relevant for any organization that accepts credit card payments.
https://www.pcisecuritystandards.org/

PPRA: The Protection of Pupil Rights Amendment affords parents and minor students' rights regarding our conduct of surveys, collection and use of information for marketing purposes, and certain physical exams.
https://studentprivacy.ed.gov/faq/what-protection-pupil-rights-amendment-ppra

New Hampshire State RSA 189:65-189:68: Student and Teacher Information Protection and Privacy as defined by the following sections:

- NH RSA 189:65 (http://www.gencourt.state.nh.us/rsa/html/XV/189/189-65.htm) Definitions
- NH RSA 189:66 (http://www.gencourt.state.nh.us/rsa/html/XV/189/189-66.htm) Data Inventory and Policies Publication
- NH RSA 189:67 (http://www.gencourt.state.nh.us/rsa/html/XV/189/189-67.htm) Limits on Disclosure of Information
- NH 189:68 (http://www.gencourt.state.nh.us/rsa/html/XV/189/189-68.htm) Student Privacy
- NH RSA 189:68-a (http://www.gencourt.state.nh.us/rsa/html/XV/189/189-68-a.htm) Student Online Personal Information

NH Minimum Standards for Privacy and Security of Student and Employee Data

New Hampshire State RSA Chapter 359-C Right to Privacy:

- NH RSA 359-C:19 (http://www.gencourt.state.nh.us/rsa/html/xxxi/359-c/359-c-19.htm) Notice of Security Breach - Definitions
- NH RSA 359-C:20 (http://www.gencourt.state.nh.us/rsa/html/xxxi/359-c/359-c-20.htm) Notice of Security Breach Required
- NH RSA 359-C:21 (http://www.gencourt.state.nh.us/rsa/html/xxxi/359-c/359-c-21.htm) Notice of Security Breach Violation

Appendix C - Digital Resource Acquisition and Use

The purpose of the Digital Resource Acquisition and Use process is to:

- ensure proper management, legality and security of information systems
- increase data integration capability and efficiency
- minimize malicious code that can be inadvertently downloaded

New Resource Acquisition

Staff will be required to complete an online request form for any new digital resources that either has an associated cost or collects staff or student data. All staff must adhere to the following guidelines regarding digital resource acquisition:

- Contracts for any system that creates, collects or uses personally identifiable information (PII), student records or confidential data must be reviewed by the ISO prior to initiation. Staff should speak with their building Principal before using ANY new app/online tool with students and seek their assistance with the evaluation/vetting process. This includes any online tool that a student interacts with where they may be creating content and/or any site that requires any student login.
- It is the responsibility of the staff requesting to use new digital content to properly vet the resource to ensure that it meets district business objectives, is in line with curriculum or behavioral standards, is age appropriate, is instructionally sound, and is appropriate for the intended use.
- Digital resources that accompany adopted instructional and/or curriculum materials will be vetted by the Curriculum Director and the Director of Technology, or designee, prior to purchase.

All new resources shall be properly evaluated against the following criteria, when applicable:

- Impact on technology environment including storage and bandwidth
- Hardware requirements, including any additional hardware
- License requirements/structure, number of licenses needed, and renewal cost
- Maintenance agreements including cost
- Resource update and maintenance schedule
- Funding for the initial purchase and continued licenses and maintenance
- Evaluate terms of service, privacy policy, and MOU/contract that meet the following criteria:
    - o The district continues to own the data shared, and all data must be available to the district upon request.
    - o The vendor's access to and use of district data is limited; the data cannot be used for marketing, targeted advertising or data mining; and the data cannot be shared with third parties unless allowed by law and authorized by the district. If metadata is collected, it will be protected to the same extent as the district's confidential or critical information.
    - o District data will be maintained in a secure manner by applying appropriate technical, physical and administrative safeguards to protect the data.
    - o The provider will comply with district guidelines for data transfer or destruction when contractual agreement is terminated.
    - o No API will be implemented without full consent of the district.
    - o All data will be treated in accordance to federal, state and local regulations
    - o The provider assumes liability and provides appropriate notification in the event of a data breach.

    Note: Exceptions can be made by the ISO when all the criteria cannot be met for a legitimate reason while still meeting all regulatory requirements for use. Parent permission may be requested from parents during the yearly online registration process for district vetted and approved applications and tools.

Approved Digital Resources

In order to ensure that all digital resources used meet security guidelines and to prevent software containing malware, viruses, or other security risk, digital resources that have been vetted are categorized as Approved or Denied.

- A list of vetted software will be maintained within the Technology Department
- It is the responsibility of staff to submit a request to use a new digital resource if a resource is not listed.
- Digital resources that are denied or have not yet been vetted will not be allowed on district owned devices or used as part of district business or instructional practices.

Digital Resource Licensing/Use

All computer software licensed or purchased for district 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.

All staff must adhere to the following guidelines regarding digital resource licensing/use:

- Only approved district resources are to be used.
- District software licenses will be:
    - kept on file in the technology office.
    - accurate, up to date, and adequate.
    - in compliance with all copyright laws and regulations.
    - in compliance with district, state and federal guidelines for data security.
- Software installed on Monadnock Regional School District systems and other electronic devices will have a current license on file or will be removed from the system or device.
- Resources with or without physical media (e.g. downloaded from the Internet, apps, or online) shall still be properly vetted and licensed, if necessary, and is applicable to this procedure.
- Under no circumstances can staff act as a parental agent when creating student accounts for online resources; resources requiring this permission must be approved at the district level.

Appendix D - Data Security Checklist

A thorough risk analysis of all Monadnock Regional School District data networks, systems, policies, and procedures shall be conducted on an annual or biennial basis or as requested by the Superintendent or ISO. The risk analysis will include internal and external vulnerability cybersecurity risk assessments and may include external penetration testing of the District network. An internal audit of District network security will be conducted annually by District Technology staff.

The Data Security Checklists examine the types of threat that may affect the ability to manage and protect the information resource. The analysis also documents any existing vulnerabilities found within each entity, which could potentially expose the information resource to threats. Finally, the analysis includes an evaluation of the information assets and the technology associated with its collection, storage, dissemination and protection.

From the combination of threats, vulnerabilities, and asset values, an estimate of the risks to the confidentiality, integrity and availability of the information is determined. The product of the risk analysis will be referred to as the risk assessment. The risk assessment shall be used to develop a plan to mitigate identified threats and risk to an acceptable level by reducing the extent of vulnerabilities.

Data Security Checklist for District Hosted Systems

□ Inventory and classification of data on system

□ Types of potential threats (internal, external, natural, manmade, electronic and non-electronic)

□ Physical security of system

□ Location within network including network systems protection (firewall, content filter) and if system is externally facing or only allows for district network access

□ Access controls including password security (can district password requirements be enforced)

□ Authentication methods (LDAP/Active Directory, Single Sign On, District managed account, user managed account)

□ Server/system security patch frequency

□ Ability to access from mobile devices

□ Ability to maintain critical system event logs

□ Ability to receive notification for critical system events

Data Security Checklist for Provider Hosted Systems

□ Inventory and classification of data on system

□ Types of potential threats (internal, external, natural, manmade, electronic and non-electronic)

□ Contract, terms of service and privacy policy are current and meet district data security requirements

□ Provider has adequate data security measures including data management and incident response

□ Ability to ensure proper access controls including password security (ie- can district password requirements be enforced)

□ Authentication methods (LDAP/Active Directory, Single Sign On, District managed account, user managed account)

□ Server/system security patch frequency

□ Ability to access from mobile devices

□ Notification practices in the event of a system compromise or security breach

Appendix E - Data Classification Levels

Personally Identifiable Information (PII)

PII is information about an individual maintained by an agency, including:

- Any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records.
- Any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Unauthorized or improper disclosure, modification, or destruction of this information could violate state and federal laws, result in civil and criminal penalties, and cause serious legal implications.

Confidential Information

Confidential Information is very important and highly sensitive material that is not classified as PII. This information is private or otherwise sensitive in nature and shall be restricted to those with a legitimate business need for access. Examples of confidential information may include: student records, personnel information, key financial information, proprietary information, system access passwords and encryption keys.

Unauthorized disclosure of this information to individuals without a business need for access may violate laws and regulations, or may cause significant consequences for district, its staff, parents, students or other stakeholders. Decisions about the provision of access to this information shall always be cleared through the data manager and/or ISO.

Internal Information

Internal Information is intended for unrestricted use within the district and in some cases within affiliated stakeholders. This type of information is already widely-distributed within the district, or it could be distributed within the organization without advance permission from the information owner. Examples of Internal Information include internal policies and procedures and handbooks.

Unauthorized disclosure of this information to outsiders may not be appropriate due to copyright, legal or contractual provisions.

Directory Information

Directory Information is information contained in an education record of a student that generally would not be considered harmful or an invasion of privacy if disclosed without the consent of a parent or eligible student. The Monadnock Regional School District designates the following items as directory information:

- Students name, address, telephone number, and dates of enrollment;
- Parents/guardians name(s) and address(es);
- Students grade level, enrollment status and dates of attendance;
- Student photographs;
- Students participation in recognized school activities and sports;
- Weight and height of members of athletic teams;
- Post-high school plans;
- Students diplomas, certificates, awards and honors received.

This information may only be disclosed as permitted in School Board Policy JRA and JRA-A

Public Information

Public Information has been specifically approved for public release by the Superintendent or appropriate district administrator. Examples of public information may include patron mailings and materials posted to the district’s website.

This information may be disclosed outside of the district.

Appendix F - Securing Data at Rest and Transit

All staff and students that log into a district owned computer will be provided with several options for data storage and transmission. Staff and students will need to ensure that they are securely storing their data. Staff and students will be able to store data on the local device. It is important to note that this data is not a part of the district's continuity plan, and thus will not be backed up by the district's backup solution. Staff and students will also have a mapped personal folder. This folder acts as a redirection of document and desktop folders to district file servers. Access to these files is restricted to the folder's owner (staff or student who is assigned) and district enterprise administrator accounts. Staff and students using Chromebook devices have limited local storage capabilities. Chromebook users are to store their data within their G Suite for Education Drive account.

Confidential and critical information will be saved and maintained in a secure manner using encryption or other password-protected security measures. Likewise, when data is transmitted, the district will use encryption or password-protected security measures.

Cloud Storage and File Sharing

The term "Cloud Storage" is used to define all types of remote server storages accessed by users through the internet. All staff and students are provided with a G Suite for Education account that provides unlimited storage. Users are responsible for all digital content on their district provided G Suite for Education Drive. When using cloud storage, staff must adhere to the following guidelines:

- Staff and students may not access cloud storage through third party applications outside of approved internet browsers and Google Drive App on Android & iOS. This will ensure that native operating systems do not replace cloud sharing security.
- Users need to be aware of default sharing settings on folders when they upload files. Users are required to limit sharing files to an as needed basis.
- Staff and students must ensure that any cloud storage providers used are approved by the district and meet district student data and data security standards.
- When exiting the district, students should responsibly copy their content to their own personal storage solution.
- When exiting the district, staff are prohibited from copying content that contains confidential information, student records or data.
- Data with personally identifiable information of staff or students may be posted to users' district provided Google Drive with appropriate security settings. Users may not post this data to other cloud sharing platforms without consent of district administration.
- Staff should never post any documents labeled classified, confidential, or restricted to any cloud storage including district provided Google Drive accounts without district approval.
- All users shall immediately report any cloud storage security problems of the district's technology resources to a teacher or administrator.
- Attempting to gain or gaining unauthorized access to cloud storage or the files of another is prohibited.
- As with other forms of district technology, district staff, students, and other G Suite for Education drive users have no expectation of privacy on data stored on this platform.

The term "File Sharing" is used to define all activities that share access to digital information whether in the cloud or on district administered mapped drives. When file sharing, staff must adhere to the following guidelines:

- Users must abide by all policies and procedures regarding professional conduct and communication when sharing, reviewing, updating, commenting and re-sharing.
- When sharing content, users must ensure that other users accessing the information in the

files have appropriate access to the information based on job function.

- All users shall immediately report any inappropriate sharing of the district's technology resources to an administrator.

External Storage Devices

The term "External Storage Devices" is used to define all portable storage devices (including USB drives, rewritable CD/DVD, memory cards, and external hard drives) used by staff and students. While the district recognizes the advantages for staff and students to maintain information on these devices, users are strongly encouraged to rely on their district provided G Suite for Education Drive account for all storage needs. When using external storage devices, staff must adhere to the following guidelines:

- Users are responsible for all content on external storage devices that have been connected to district technology resources.
- Users must ensure that they will not introduce harmful software including computer viruses, malware, non-district approved software, or hacking tools to district technology resources.
- Users must ensure that the data will remain secure through appropriate encryption or password protection when transferring files containing PII or protected information to an external storage device. Users should only keep the information stored on the external device for the duration of the project, and then promptly remove.
- Staff should never transfer any documents labeled classified, confidential, or restricted to any external storage device.
- Staff should never transfer or create confidential data or student records on personal storage devices.

File Transmission Practices

- Staff are responsible for securing sensitive data for transmission through email or other channels. When possible, staff should de-identify or redact any PII or confidential information prior to transmission.
- Staff should never include a password in any electronic communication unless directed to do so by Technology Staff.
- Staff should not transmit files labeled classified, confidential, or restricted through email or third party file transfer services without district approval.
- Regular transmission of student data to services such the District Library Management system, Food Service Management system and Single Sign On Provider system is managed by the technology department using a secure data transfer protocol. All such services are approved by a district/building administrator and the Director of Technology.

Credit Card and Electronic Payment

Users of systems that process electronic payments, including but not limited to processing credit card information, must adhere to strict guidelines regarding the protection of payment information and cardholder data. These users are responsible for adhering to the following requirements and appropriate level of PCI compliance when handling such data:

- Never store cardholder data on district systems or in written form. All cardholder data may only be entered in secured payment systems approved by the district. Any cardholder data collected in written form must be shredded immediately after entry into approved system.
- The district will never maintain a data system for payment information. All payment information will be stored and processed by a 3rd party accessible through a secure portal.
- Never request cardholder information to be transmitted via email or any other electronic communication system.
- Payment information shall be entered directly into the approved payment system by individual making payment. If the individual is not able to directly input the payment, designated staff may gain

verbal approval for the payment process either in person or via phone (after identification is verified). If verbal payment information is received, that information must be entered directly into the payment system and not written down during the process.

• If payment information is collected via a physical form, that form must be shredded or payment information redacted immediately upon receipt and entry into payment system.

Appendix G - Physical Security Controls

The following physical security controls shall be adhered to:

- Network systems shall be installed in an access-controlled area. The area in and around the computer facility shall afford protection against fire, water damage, and other environmental hazards such as power outages and extreme temperature situations.
- Monitor and maintain data centers' temperature and humidity levels.
- File servers and/or storage containing PII, Confidential and/or Internal Information shall be installed in a secure area to prevent theft, destruction, or access by unauthorized individuals.
- Ensure network systems and network equipment are properly secured to prevent unauthorized physical access and data is properly safeguarded to protect from loss.
- Computers and other systems shall be secured against use by unauthorized individuals. It is the responsibility of the user to not leave these devices logged in, unattended, and open to unauthorized use.
- Monitor and control the delivery and removal of all data-storing technological equipment or systems. Maintain a record of all such items entering or exiting their assigned location using the district approved technology inventory program. No technology equipment regardless of how purchased or funded shall be moved without the explicit approval of the technology department.
- Ensure that technological equipment or systems being removed for transfer to another organization or being designated as surplus property is appropriately sanitized in accordance with applicable policies and procedures (see Appendix H: Asset Management).

Appendix H - Asset Management

Data security must be maintained through the life of an asset, including the destruction of data and disposal of assets. Any computer, laptop, mobile device, printing and/or scanning device, network appliance/equipment, AV equipment, server, internal or external storage, communication device or any other current or future electronic or technological device may be referred to as a system, asset or device.

All involved systems and information are assets of the district and are expected to be protected from misuse, unauthorized manipulation, and destruction.

Inventory

All technology devices or systems considered an asset are inventoried by the technology department. This includes, but is not limited to, network appliances, servers, computers, laptops, mobile devices, and external hard drives. The technology department will conduct annual inventory verification of all district devices. It is the responsibility of the technology department to update the inventory system to reflect any in-school transfers, in-district transfers, or other location changes for district technology assets.

Disposal Guidelines

Assets shall be considered for disposal in accordance with state/federal regulations and School Board Policy DN. The following considerations are used when assessing an asset for disposal:

- End of useful life
- Lack of continued need
- Obsolescence
- Wear, damage, or deterioration
- Excessive cost of maintenance or repair
- Salable value

The Director of Technology shall approve disposals of any district technology asset.

Methods of Disposal

Once equipment has been designated and approved for disposal (does not have salable value), it shall be handled according to one of the following methods. It is the responsibility of the technology department to update the inventory system to reflect the disposal of the asset.

Discard

All technology assets shall be discarded in a manner consistent with applicable environmental regulations. Electronic equipment may contain hazardous materials such as mercury, lead, and hexavalent chromium. When possible, any reusable hardware that can't be used as parts to repair and/or maintain district technology assets shall be removed (motherboards, screens, adapters, memory). In addition, systems may contain Personally Identifiable Information (PII), Confidential, or Internal Information. Systems shall be wiped clean of this information prior to leaving the school district.

A district-approved vendor shall be contracted for the disposal of all technological systems/equipment. The vendor shall provide written documentation verifying the method used for disposal and a certificate stating that no data of any kind can be retrieved from the hard drive or any other component capable of storing data.

Under no circumstances should any technological systems/equipment be placed in the trash.

Donation/Gift

In the event that the district determines that an asset shall be donated or gifted, systems shall be wiped clean of Personally Identifiable Information (PII), Confidential, and/or Internal Information prior to leaving the school district. The Monadnock Regional School District will not support or repair any equipment that is donated. In addition, software licenses are not transferred outside the district. Therefore, systems must be returned to factory installation, or drives shall be removed and discarded prior to donation.

Appendix I - Virus, Malware, Spyware, Phishing and SPAM Protection

Virus, Malware, and Spyware Protection

Monadnock Regional School District PC desktops, laptops, and file servers are protected using enterprise virus / malware / spyware software. Definitions are updated daily and an on-access scan is performed on all “read” files continuously. All files and systems are scanned.

Internet Filtering

Student learning using online content and social collaboration continues to increase. The Monadnock Regional School District views Internet filtering as a way to balance safety with learning, letting good content, resources, and connections in while blocking the bad. To balance educational Internet resource and application use with student safety and network security, the Internet traffic from all devices on the district network is routed through the district firewall and content filter. Filtering levels are based on the role of the user, staff or student and student grade level. All sites that are known for malicious software, phishing, spyware, etc. are blocked.

Phishing and SPAM Protection

Email is filtered for viruses, phishing, spam, and spoofing using Google services.

Security Patches

Server patch management is performed regularly. Security patches are applied on an as needed basis, but at least biweekly.

Appendix J - Account Management

Access controls are essential for data security and integrity. The Monadnock Regional School District maintains a strict process for the creation and termination of district accounts. All new staff accounts are authorized through an HR hiring process prior to creation. Role-based permissions are used to establish access to all systems. Access security is audited at least annually or whenever access permission requirements are changed for a particular application/software or when an application/software is no longer necessary.

Staff Accounts

When a staff member is hired by the Monadnock Regional School District, the following process ensures that each staff member has the correct access and permissions to the resources that are required for their position.

- Notification of new staff member is sent from Human Resources to the Technology Department. This notification includes position, building assignment(s), and start date.
- Only after notification has been received from Human Resources, the Technology Department creates user accounts. The user is given access and permissions to the necessary resources based on their position and building assignment(s) (see Appendix K: Data Access Roles and Permissions).
- Any exception to permissions must be approved by the district administrator responsible for the system (data manager) and the Director of Technology.

When a staff member's employment is ended, either by termination or resignation, account permissions are revoked in one of two ways.

- In the event of termination, HR will notify the Technology Department via email or phone call requiring the account to be disabled at once, preventing any further access to district resources.
- In the event of resignation, HR will notify the Technology Department via email indicating the termination date. The account is disabled at the end of business on the termination date, preventing further access to district resources.
- In the event that a user having elevated permissions to any system separates from the district, additional measures are taken to ensure that all elevated accounts to those systems are secure.

Local/Domain Administrator Access

Only members of the District Technology staff will be granted access to domain level administrator and local machine administrator accounts in order to complete their job functions.

Remote Access

Access into the District's network from outside is strictly prohibited without explicit authorization from the ISO. Remote access will be granted through virtual private network (VPN) connection through the district's network VPN appliance; no other method of remote access shall be granted without explicit authorization from the ISO. PII, confidential information and/or Internal Information that is stored or accessed remotely shall maintain the same level of protection as information stored and accessed within District's network.

In the event that VPN access is needed by a contractor/vendor, access must be approved by the ISO. The Network Administrator will establish the contractor account, only granting access to the server/application that the contractor/vendor supports.

All VPN accounts will be reviewed at least annually.

Contractors/Vendors

Access to contractors/vendors is governed through the same process using School Board Policy EHAB. All contractor/vendor access must be approved by HR and ISO. All contractors doing business on district premises must also pass a background check unless other security measures are addressed in a vendor contract. All contractors/vendors accessing district data will be considered on premise users. Once the approval has been obtained, the technology department will create the account.

Appendix K - Data Access Roles and Permissions

Student Information System (SIS)

Staff are entered into the Monadnock Regional School District's student information system. Only staff whose roles require access are provided accounts for the system. The following minimum information is entered for each staff member:

- Building/Site location
- Status - Active
- Staff Type
- District Email Address
- Primary Alert Phone Number and Cell phone number

Access accounts for the District's SIS are setup based on staff role/position, building and required access to student data and are assigned by the Director of Technology or designee. Teacher accounts are created for all staff responsible for taking student attendance and entering and maintaining grades. Teacher accounts login to the SIS Teacher Portal. Staff assigned a Teacher account only have access to students they teach or provide services to. Administrative accounts are created based on the staff member's role/position and function and further restrictions to data are controlled through security groups. Security groups control access permissions to certain data sets such as attendance, demographic data, grades, discipline etc. and whether the staff member can view or maintain data. Additional page level permissions are assigned to the security groups. Administrative accounts log into the SIS Admin Portal.

Financial System

All staff members are entered into the District's financial system for the purpose of staff payroll and HR tracking. Staff access to their individual payroll information is granted through the employee portal. Only staff requiring access are provided accounts for the financial/personnel system.

After basic information and user ID are created, a security role is assigned to the account granting them access to designated areas of the financial system to complete their job responsibilities.

Special Education System

The State of New Hampshire provides the District access to the NH Special Education Information System (NHSEIS) that houses all student IEP information. Access accounts to NHSEIS is maintained by the District's Director of Special Services office through the MyNHDOE single sign on portal. A user role determines the user's authority and applicable permissions within the NHSEIS system. The established roles are as follows:

- School Administrator
- Provider
- Case Manager
- District IT Administrator
- IEP Team Member
- District Administrator
- SAU System Administrator
- SAU System Staff
- General Ed Teacher
- SAU District Administrator

The following user roles access NHSEIS through the MyNHDOE portal: Case Manager, District Administrator, District IT Administrator, SAU District Administrator, SAU System Administrator, SAU

System Staff, and School Administrator. The remaining user roles, Provider, General Ed Teacher and IEP Team Member access NHSEIS through a SAU specific web address.

Health Software System

School District Nurses, Nurse Substitutes and Technology Staff are the only staff members granted access to the District's Health Software system. Technology Staff access is for the purpose of upgrades, and technical support for the use of the system. The medical data that is collected and maintained by the school nurses on the system includes immunizations, conditions, medications, and clinic logs (Time in/out of clinic and action taken). School nurses are the only accounts that can view and maintain medical information.

Food Services System

The District uses a Food Services software management system to track data and perform functions necessary for the efficient operation of the Food Service Program. Food service staff are granted accounts with access to only the parts of the system that are necessary to complete their job functions. Technology Staff access is for the purpose of upgrades, and technical support for the use of the system and cash registers. Strict security roles and permissions are in place to ensure that confidential information is only viewable by authorized staff.

Appendix L - Passphrase/Password Security

Passphrase’s are generally longer than a password, and can contain spaces such as: “The sun will come out tomorrow!”.

- Passphrases can be much easier to remember. The user has the ability to choose a sentence, the user can make it logical. By doing this, the users will not have to try and remember a random mix of special characters, numbers, and upper/lowercase letters.
- Passwords are becoming much easier to crack due to technological advances.
- Passphrases are becoming supported across all major platforms.
- Most password cracking attempts just give up after the 10-character mark.

The District requires the use of strictly controlled passphrases/passwords for network access and for access to secure sites and information. All passphrases/passwords to district systems shall meet or exceed the below requirements.

- Passphrases/Passwords shall never be shared with another person.
- When possible, user created passphrases/passwords should adhere to the same criteria as required for district network access as outlined below.
- Passphrases/Passwords shall never be saved when prompted by any application with the exceptions of single sign-on (SSO) systems and password managers as approved by the Technology Department.
- Passphrases/passwords shall not be programmed into a computer or recorded anywhere that someone may find and use them.
- When creating passphrases/password for secure information or sites, it is important **not** to use passwords that are easily guessed due to their association with the user (i.e. children’s names, pets’ names, or birthdays).
- Users and staff who have reason to believe a password is lost or compromised must notify the Director of Technology or designee as soon as possible. The technology department will verify the identity of the person requesting the change before resetting the password.

District network access to resources managed through LDAP/SSO:

- Passphrases/Passwords must be “strong,” and must be a minimum of 12 characters long, must include at least one uppercase character, one lowercase character, one special character (!@#$%^&*(_+{}|[]\:”;’<>?,./)
- Passwords will only be changed in the event the user shares their password with another staff member or they believe their account has been compromised.
- Your password must not be too similar to your username.
- Do not use your district password for any non-district systems.

Where possible, system software should enforce the following passphrase/password standards:

- Passphrases/Passwords routed over a network shall be encrypted.
- Passphrases/Passwords shall be entered in a non-display field.
- System software shall enforce the changing of passwords and the minimum length.
- System software shall disable the user password when more than five consecutive invalid passwords are given.

Appendix M - Technology Disaster Recovery Plan

Objectives

The primary purpose of the Technology Disaster Recovery Plan (TDRP) is to enable the Monadnock Regional School District (Monadnock Regional) to respond effectively and efficiently to a natural disaster or critical failure of the district's data center and/or core systems. The objectives during a natural disaster or critical failure are the following:

- Minimize the loss or downtime of core systems and access to business critical data.
- Recover and restore the district's critical systems and data.
- Maintain essential technology resources critical to the day to day operations of the district.
- Minimize the impact to the staff and students during or after a critical failure.

Planning Assumptions

The following planning assumptions were used in the development of Monadnock Regional's TDRP:

- There may be natural disasters that will have greater impact than others.
- There will be factors that are beyond the department's control or ability to predict during a disaster.
- There is the possibility of complete loss of the current data center.
- We will have adequate storage to recover systems.
- District data is housed at district data center and backed up in the cloud.
- District data is hosted by 3rd party providers.
- In the event of a critical failure to network infrastructure in the datacenter, District networking may be significantly impacted.

Disaster Recovery/Critical Failure Team

The Monadnock Regional has appointed the following people to the disaster recovery/critical failure team, otherwise known as the Incident Response Team: Director of Technology, Network Administrator, IT Support Specialists, Director of Facilities and Maintenance Supervisor.

In the event the TDRP is activated, overall management of the response is delegated to this team. Their primary responsibilities include:

- Determining the impact of the natural disaster/critical failure.
- Communication of impact and or loss, and updates of progress to the Superintendent.
- Communication of outages and updates to district staff.
- Oversight of the TDRP implementation and restoration of critical systems and data.
- Allocation and management of technology staff during the event.
- Working with manufacturers and/or vendors during the recovery and restoration of critical systems and data.
- Oversight of TDRP implementation debrief.

Activation

The TDRP will be activated in the event of the following:

- A natural disaster has occurred and affects the operation of the District's data center. A natural disaster includes but is not limited to the following: tornado, earthquake, lightning, and floods.

- A fire has impacted the data center.
- Water or flooding has impacted the data center.
- Critical system failure.

The Information Security Officer (ISO) will act as the Incident Response Manager (IRM). If the ISO is not able to act as the IRM, a member of the Superintendent's Leadership Team will assume the role of the IRM, with assistance from the Incident Response Team (IRT).

Notification

The following groups will be notified in the event the plan has been activated:

- Superintendent
- Superintendent's Leadership Team
- Technology Staff
- District Staff
- Parents and Students
- Vendors

Information will be disseminated to the above groups through whichever means of communication is available at the time. This could include any one or combination of the following:

- Phone
- Email
- Social Media/Website
- Radio or Television

The TDRP team will work with the Superintendent on which information will be conveyed to each above group and what means will be used.

Implementation

The TDRP team has the following in place to bring the District back online in the least amount of time possible:

- Maintained spreadsheet listing all server names, physical and virtual, and their function.
- Maintained secure application to store all system administrator accounts, passwords and vendor contact information. This will be accessible only to applicable Technology Staff who need access to perform their job functions.

Deactivation

The TDRP team will deactivate the plan once services are fully restored.

Evaluation

An internal evaluation of the Monadnock Regional's TDRP response will be conducted. This will entail gathering documentation from the response and feedback from all stakeholders and incorporate into an after action report and corrective action plan. The result will be an update to the TDRP and other emergency response plans as appropriate.

Appendix N - Data Breach Response Plan

Objectives

The purpose of the Technology Data Breach Plan (TDBP) is to enable the Monadnock Regional School District to respond effectively and efficiently to an actual or suspected data breach involving personally identifiable information (PII), confidential or protected information, district identifiable information and other significant cybersecurity incident. The objectives of the TDBP are:

- Convene the Incident Response Team (IRT) as necessary.
- Validate and contain the data security breach.
- Analyze the breach to determine scope and composition.
- Minimize impact to the staff and students after a data breach has occurred.
- Notification of data owners, legal counsel, state/federal agencies and law enforcement as deemed necessary.

Planning Assumptions

The following planning assumptions were used in the development of Monadnock Regional School District's TDBP:

- There may be data breaches that will have greater impact than others.
- There will be factors that are beyond the department's control or ability to predict during a data breach.
- District data is backed up.
- Some District data is hosted by 3rd party providers.

Data Breach/Incident Response Team

Monadnock Regional School District has appointed the following people to the data breach/incident response team: Director of Technology and the Network Administrator.

In the event the TDBP is activated, overall management of the response is delegated to this team. Their primary responsibilities include:

- Determine the nature of the data compromised and its impact to staff, students and the district itself.
- Communicate impact, the number of affected individuals, the likelihood information will be or has been used by unauthorized individuals and updates of progress to the Superintendent and Business Administrator.
- Coordinate with Superintendent to ensure communication with district staff and or parents as deemed appropriate.
- Oversight of the TDBP implementation and data breach resolution.
- Allocate and manage technology staff resources during the event.
- Work with vendors, 3rd party providers, manufacturers, legal counsel, district data breach insurance provider, state/federal agencies and law enforcement while correcting the data breach and its repercussions.
- Oversight of TDBP implementation debrief.

Activation

The TDBP will be activated in the event of the following:

- A data breach has occurred and affects the district itself. A data breach includes but is not limited to an incident in which sensitive, protected or confidential data has potentially been viewed, stolen or used by an individual unauthorized to do so.
- Personal Health Information (PHI) has been compromised.
- Personally Identifiable Information (PII) has been compromised.
- Confidential or sensitive data has been compromised.
- Network hack/intrusion has occurred.

The Information Security Officer (ISO) will act as the incident response manager (IRM). If the ISO is not able to act as the IRM, a member of the Superintendent's Leadership Team will assume the role of IRM, with assistance from the IRT. The breach response and reporting process will be documented according to state and federal requirements. The Director of Technology will work with the Superintendent to dispense and coordinate the notification and public message of the breach.

Notification

The following groups will be notified in the event the plan has been activated:

- Superintendent
- Superintendent's Leadership Team
- Technology Staff
- District Staff
- Parents and Students
- Vendors

Information will be disseminated to the above groups through whichever means of communication deemed appropriate. This could include any one or combination of the following:

- Email
- Social Media/Website
- Radio or Television
- Written Notice
- Phone

The TDBP team will work with district leadership on which information will be conveyed to each above group, timing of that communication and what means will be used.

Implementation

The TDBP team has the following processes in place to contain the data breach in the least of amount of time possible:

- Data inventory of all systems containing sensitive data.

- Data dictionary of all district hosted information systems.

- Maintained spreadsheet listing all server names, physical and virtual, and their function.

- Maintained secure application to store all system administrator accounts, passwords and vendor contact information. This will be accessible only to applicable Technology Staff who need access to perform their job functions.

- The District's data backup solution includes the use of a backup manager and off-site file storage, which backs up data locally in the datacenter and offsite.

The following will take place during the incident response:

- The members of the IRT will be assembled once a breach has been validated. The IRT will be comprised of the Director of Technology, Network Administrator and IT Support Specialists. Additional members of the Monadnock Regional School District's administrative team and technology department may be designated to assist on the IRT.

- The IRT will determine the status of the breach, on-going, active, or post-breach. For an active and ongoing breach, the IRT will initiate appropriate measures to prevent further data loss. These measures include, but are not limited to, securing and blocking unauthorized access to systems/data and preserving any and all evidence for investigation.

- The IRT will work with the data managers and data owners to determine the scope and composition of the breach, secure sensitive data, mitigate the damage that may arise from the breach and determine the root cause(s) of the breach to devise mitigating strategies and prevent future occurrences.

- The IRM will work with legal counsel and the Superintendent's Leadership Team to determine appropriate course of action pursuant to state statute. This includes notification of the authorities, and local law enforcement.

- Collaboration between the authorities and the IRT will take place with the IRM. The IRT will work with the proper authorities to make sure any and all evidence is properly handled and preserved.

- On advice from legal counsel, an outside party may be hired to conduct the forensic investigation of the breach. When the investigation has concluded, all evidence will be safely stored, recorded or destroyed (where appropriate).

- All affected data, machines and devices will be identified and removed from the network as deemed appropriate for the investigation. Interviews will be conducted with key personnel and facts of the incident will be documented and the evidence preserved for later examination.

- The IRT will work with the Superintendent's office to outline the notification of the data owners and those affected. Communication will be sent out as directed by legal counsel and advised by the district communications team. The types of communication will include, but not limited to, email, text message, postal mail, substitute notice and/or phone call.

- The IRM, in conjunction with the IRT, legal counsel and the Superintendent's Leadership Team will determine if notification of affected individuals is necessary. Once the determination is made to notify affected individuals, a letter will be written in accordance with all federal and state statutes, and local procedures. If it is determined that identity theft or other fraud is not reasonably likely to occur as a result of the breach, such a determination shall be documented in writing and filed at the Superintendent's office.

Deactivation

The TDBP team will deactivate the plan once the data breach has been fully contained.

Evaluation

Once the breach has been mitigated an internal evaluation of the Monadnock Regional's TDBP response will be conducted. The IRT, in conjunction with the IRM and others that were involved, will review the breach and all mitigation steps to determine the probable cause(s) and minimize the risk of a future occurrence. Feedback from the responders and affected entities may result in an update to the TDBP and other emergency response plans as appropriate. Information security training programs will be modified to include countermeasures to mitigate and remediate previous breaches so that past breaches do not recur. The reports and incident review will be filed with all evidence of the breach.

Appendix O – NH Minimum Standards for Privacy and Security of Student and Employee Data

Minimum Standards for Privacy and Security of Student and Employee Data
New Hampshire Department of Education

I. Purpose & Applicability

A. This document defines minimum standards ("Standards") for the privacy and security of student and employee information for Local Education Agencies ("LEA") that the Department is required to establish according to New Hampshire Revised Statutes Annotated (RSA) 189:66, V.

B. These Standards apply to "Student Personally-Identifiable Data" and "Teacher Personally-Identifiable Data" (RSA 189:65), as well as "Covered Information" (RSA 189:68) handled by LEAs in both electronic and physical formats. Unless otherwise noted, the terms "Covered Information" shall include Student and Teacher Personally Identifiable Data throughout this document.

C. All LEAs under the purview of the New Hampshire Department of Education are required to implement these Standards. II. Minimum Privacy and Security Standards These Standards have been developed from a subset of basic and derived security requirements from National Institute of Standards and Technology Special Publication 800-171 Revision 1, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations." More information about each security standard can be found at the reference listed from NIST SP 800-171. LEAs are encouraged to review and incorporate additional security requirements from NIST SP 800-171, as appropriate.

A. Access Control

1. Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems). (NIST SP 800-171: 3.1.1)
2. Limit system access to the types of transactions and functions that authorized users are permitted to execute. (NIST SP 800-171: 3.1.2)
3. Employ the principle of least privilege, including for specific security functions and privileged accounts. (NIST SP 800-171: 3.1.5)
4. Limit unsuccessful logon attempts. (NIST SP 800-171: 3.1.8)
5. Employ cryptographic mechanisms to protect the confidentiality of remote access sessions. (NIST SP 800-171: 3.1.13)
6. Authorize wireless access prior to allowing such connections. (NIST SP 800-171: 3.1.16)
7. Protect wireless access using authentication and encryption. (NIST SP 800-171: 3.1.17)

B. Awareness and Training

1. Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems. (NIST SP 800-171: 3.2.1)
2. Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities. (NIST SP 800-171: 3.2.2)

C. Audit and Accountability

1. Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity. (NIST SP 800-171: 3.3.1)
2. Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions. (NIST SP 800- 171: 3.3.2)

D. Configuration Management

1. Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. (NIST SP 800-171: 3.4.1)
2. Establish and enforce security configuration settings for information technology products employed in organizational systems. (NIST SP 800-171: 3.4.2)
3. Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services. (NIST SP 800-171: 3.4.7)

E. Identification and Authentication

1. Identify system users, processes acting on behalf of users, and devices. (NIST SP 800-171: 3.5.1)
2. Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems. (NIST SP 800-171: 3.5.2)
3. Enforce a minimum password complexity and change of characters when new passwords are created. (NIST SP 800-171: 3.5.7)

F. Incident Response

1. Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities. (NIST SP 800-171: 3.6.1)
2. Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization. (NIST SP 800-171: 3.6.2)

G. Maintenance

1. Perform maintenance on organizational systems. (NIST SP 800-171: 3.7.1)
2. Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance. (NIST SP 800-171: 3.7.2)
3. Ensure equipment removed for off-site maintenance is sanitized of any Covered Information in accordance with NIST SP 800-88 Revision 1. (NIST SP 800-171: 3.7.3)

H. Media Protection

1. Protect (i.e., physically control and securely store) system media containing Covered Information, both paper and digital. (NIST SP 800-171: 3.8.1)
2. Limit access to Covered Information on system media to authorized users. (NIST SP 800-171: 3.8.2)
3. Sanitize or destroy system media containing Covered Information in accordance with NIST SP 800-88 Revision 1 before disposal or release for reuse. (NIST SP 800-171: 3.8.3)
4. Control access to media containing Covered Information and maintain accountability for media during transport outside of controlled areas. (NIST SP 800-171: 3.8.5)

I. Personnel Security

1. Screen individuals prior to authorizing access to organizational systems containing Covered Information. (NIST SP 800-171: 3.9.1)
2. Ensure that organizational systems containing Covered Information are protected during and after personnel actions such as terminations and transfers. (NIST SP 800-171: 3.9.2)

J. Physical Protection

1. Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals. (NIST SP 800-171: 3.10.1)
2. Protect and monitor the physical facility and support infrastructure for organizational systems. (NIST SP 800-171: 3.10.2)

K. Risk Assessment

1. Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of

Covered Information. (NIST SP 800-171: 3.11.1)

2. Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified. (NIST SP 800-171: 3.11.2)
3. Remediate vulnerabilities in accordance with risk assessments. (NIST SP 800-171: 3.11.3)

L. Security Assessment

1. Periodically assess the security controls in organizational systems to determine if the controls are effective in their application. (NIST SP 800-171: 3.12.1)
2. Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems. (NIST SP 800- 171: 3.12.2)
3. Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls. (NIST SP 800-171: 3.12.3)

M. System and Communications Protection

1. Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems. (NIST SP 800-171: 3.13.1)
2. Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception). (NIST SP 800-171: 3.13.6)
3. Protect the confidentiality of Covered Information at rest. (NIST SP 800- 171: 3.13.16)

N. System and Information Integrity

1. Identify, report, and correct system flaws in a timely manner. (NIST SP 800-171: 3.14.1)
2. Provide protection from malicious code (i.e. Antivirus and Antimalware) at designated locations within organizational systems. (NIST SP 800-171: 3.14.2)
3. Monitor system security alerts and advisories and take action in response. (NIST SP 800 171: 3.14.3)
4. Update malicious code protection mechanisms when new releases are available. (NIST SP 800-171: 3.14.4)

Monadnock Regional School District (MRSD)
School Board Meeting Minutes
May 2, 2023
MRMHS Library/Zoom, Swanzey, NH

Members Present: Kristen Noonan, Scott Peters, Dan LeClair, Brian Bohannon via Zoom, Eric Stanley, Edmond LaPlante, Betty Tatro, Lisa Steadman and Stephanie Lawlor. **Absent:** Cheryl McDaniel-Thomas, Nick Mosher, Jennifer Strimbeck and Jeff Cesaitis.

Administration Present: J. Rathbun, Assistant Superintendent and J. Morin, Business Administrator.

1. **CALL THE MEETING TO ORDER at 6:30 PM.** The Board did not have a quorum**.**
2. **Non-Public RSA 91-A:3, II (c) Manifest Hardship Hearing:** The family did not arrive for the manifest hardship hearing.
3. **CALL THE MEETING TO ORDER at 6:45 PM.** S. Peters called the meeting to order.
4. **PUBLIC COMMENTS:** There were no public comments.

5. **#CelebrateMRSD:**

a. S. Peters reminded the Board Members who would be attending the Retirement/Awards Dinner to RSVP to L.Sutton.

b. J. Rathbun reported that MTC will be holding the NHDI Residency Program as well as a Kindergarten Ice Cream Social. The Senior Class will hold Breakfast with Pando. With the use of the CARES Funds Cutler students were able to visit the Seacoast Center and the Boston Museum of Science. ***B. Bohannon arrives via Zoom.***

c. **Staff Appreciation Week:** J. Rathbun explained that swag has been ordered for all of the staff and it will be delivered next week.

6. **MATTERS FOR INFORMATION & DISCUSSION:**

a. **Q3 Education Report:** J. Rathbun would like to present the Q3 Education Report at the joint meeting with the Budget Committee. He will also talk about where we are district - wide not only academics but plans and concerns.

J. Rathbun explained that we need to look at the health and wellness of the students. Things are different NH has expectations. Currently the guidance special is done by a school counselor every week. The administration would like to propose creating a specialist guidance position. This proposed position will give opportunity to focus on the new expectations from the State and free up the school counselors. ***J. Morin arrives.***

b. **Federal Funds General Assurance:** J. Rathbun explained that this was reviewed at the last meeting but L. Steadman and S.Peters did not sign and date the document on a School Board Meeting day. It needs to be signed tonight. The Assurance is to accept the Federal funds and all of the DAF Policies, to comply with the policies and to follow all federal laws.

c. FY22 Audit Recap: S. Peters explained that the FY22 Audit was in the packet. J. Morin explained the audit is received each year. She explained there is a letter in the packet that gives the highlights. She said everything they found is normal in the course of a school district. She mentioned the manifest not having a quorum signing it and comments on the disbursement of student activity funds. It is a matter of getting into the new process. The school year is almost over. It is too late to implement new changes. J.Morin commented that the Business office did a great job following procedure and the schools did great with the changes asked of them. ***D. LeClair arrives.***

d. CCC Regional Agreement: The draft of the CCC Regional Agreement was in the packet. It was explained that the State will only allow 10 conflicting calendar days. It was mentioned that Keene, Fall Mtn.and Monadnock need to work together to form the calendar. The CCC follows the Keene High School Calendar. J. Rathbun explained there are 5 conflicting days due to Keene's early release days. It was mentioned that the number of Monadnock students has increased but Keene has a larger number of students. The CCC representative was in attendance at Career Day. J. Rathbun explained Monadnock is not a receiving district. He would like to provide a welding class, forest management and ATV Repair for the students and have students from other districts attend Monadnock, such as the CCC. K. Noonan explained that students can earn up to 12 credits through the LNA Program at the CCC. B.Tatro mentioned that N. Carney from the Budget Committee teaches a course at the CCC

e. Preparing for Joint Meeting with BudgetCommittee on 5/16/23: S.Peters explained that the Board and the Budget Committee will be having an extra joint meeting on May 16, 2023 and also hold the joint meeting in November. S.Peters said that he and A. Hopkins have connected and started working on an agenda. The Board reviewed the proposed agenda. J. Morin explained that there will be a first interest only payment on the bond and then a full one to follow. She does not feel there will be a year in which there is no payment. S. Peters proposed adding an Education Committee overview to the agenda. It was commented that the committee needs to discuss attendance, behavior and parent participation not only proficiency. The whole package. It was suggested that the Budget Committee attend the Board Meetings regarding the test results. B. Tatro commented that the Budget Committee would like an executive summary. J. Rathbun explained that the test was created by a company to make money. It is only one test. The Budget Committee is looking for proficiency. B.Tatro explained that the Budget Committee feels that they should be equal to the Board and not a subcommittee. S. Peters commented that they have been excellent partners. K. Noonan commented that she hopes that the Budget Committee knows that we cannot talk specifics regarding the negotiations.

f. Overview of Critical Staffing Shortage (State of NH Definition +MRSD Current Status): The Board received information from the administration regarding the critical staffing shortage. J. Rathbun commented that the administration is feeling much better than last year. There are 44 vacancies for next year. J. Rathbun explained that the critical staffing shortage list comes from the State. The State asks districts to share the vacancy list and they decide the shortage and identify alternative hiring. Certified staff are the only group on the critical shortage list. J. Rathbun explained Alternative 4 and Alternative 5.

7. MATTERS THAT BOARD ACTION:

a. Rules for Board Member Remote Participation: S. Peters explained that Policy BBAB states that if the Board Member is attending the meeting remotely the member has to state the reason why and it needs to be stated in the meeting minutes. Policy BEDDA Rules for Remote Participation was presented to the Board. S.Peters presented edits to the policy referring to remote participation. **MOTION:** S.Peters **MOVED** to refer the proposed remote participation changes to the Policy Committee. **SECOND:** S. Lawlor. **VOTE:** 8.731/0/0/4.269. **Motion passes.**

b. April 18, 2023 Meeting Minutes: MOTION: K. Noonan **MOVED** to approve the April 18, 2023 Public and Non-Public Meeting Minutes as presented with an addition to 5.a. Describing the question asked about the waiting list and to have non-public “1” be relabeled as non-public b. **SECOND:** S.Lawlor **DISCUSSION:** L. Steadman asked for clarity regarding the April 4, 2023 Minutes because she was not present. She asked if the students on the Preschool waiting list are regular ed. Students or Special ed. Students. **VOTE:** 8.605/0/1.126/4.269. **Motion passes.**

c. Manifest: MOTION: L.Steadman **MOVED** to approve the manifest in the amount of $1,381,713.06 as presented by the administration. **SECOND:** B. Tatro **VOTE:** . **Motion passes.**

d. Budget Transfer: J. Morin presented 5 budget transfers to the Board. L. Spencer has requested a budget transfer in the amount of $29,400 from the Regular Instruction Salaries line to the Other Purchased Property Services line to purchase and installation of Air Quality Sensors at MRMHS, L.Stevens and J. Morin have requested a budget transfer in the amount of $20,659 from multiple Special Ed. salary and benefits lines and multiple Regular Ed. salary and benefits line to hire a paraprofessional to support Kindergarten, not related to Special Ed., J. Morin has requested a budget transfer in the amount of $11,100 from the Special Education Health Ins. line to the Building and Grounds Health Ins.line for a change in position/staffing, needs to move benefits with the person, T. Givetz has requested a budget transfer in the amount of $8250 from the Regular Instruction Salaries line to the Replacement Furn/Equipment line to purchase 2 tables, 2 Art tables and chair replacement and a budget transfer request from K. Stone in the amount of $11,360 from the Regular Instruction Health Insurance line to the Replacement Furn/Equipment line to purchase 4 cafeteria tables. **MOTION:** L. Steadman **MOVED** to approve the budget transfers as presented by J. Morin. **SECOND:** K. Noonan. **DISCUSSION:** J. Morin explained that the staff making the request obtain a quote and the items are not ordered until the School Board approves the budget transfer. The amount being transferred between lines may not be the entire amount of the purchase. If the District had a default budget the amount would be pre-budget transfers. **VOTE:** 8.731/0/0/4.269. **Motion passes.** ***D. LeClair arrives.***

e. Superintendent Search: The Board received a boilerplate from the NHSBA. This proposal is not for the current year and has not been updated. J. Rathbun suggested NESDEC to help with the search. S. Peters commented that the Board should be ready in a month to start the process. B. Bohannon and S. Lawlor suggested a national search. S.Peters said he has not asked the NHSBA how wide their search would be. J. Rathbun explained the candidate must have NH credentials. K. Noonan said that she is comfortable with the NHSBA. We have a great working relationship with them. K. Noonan, B. Bohannon, L.Steadman, B. Tatro and S. Lawlor volunteered to be on the Search Committee. **MOTION:** B. Bohannon **MOVED** to create documentation describing the desired attributes of a Superintendent. **SECOND:** S. Lawlor. **VOTE:** 9.863/0/0/3.317. **Motion passes.** S.Peters suggested a deadline of June 30, 2023.

f. Charter & Goals: Finance/Facilities: B.Tatro explained that Chart and Goals will be in the next Board packet.

g. Charter & Goals: Policy: Policy has not met.

h. Charter & Goals: Education: S. Lawlor reported that the committee met and had a great discussion. The committee has a number of questions to ask the administration in order to proceed. The next step is to have an interview with the administration. The committee presented the Committee Charter to the Board. **MOTION:** S. Lawlor **MOVED** to approve the Ed/Tech Committee Charter as presented. **SECOND:** Tatro. **VOTE:** 9.863/0/0/3.137. **Motion passes.** The Ed/Tech Goals were presented to the committee. The committee explained that they had a healthy conversation regarding the goals. The committee needs questions answered before they answer what the strategy is. B.Tatro suggested it may be an approach instead of a strategy. **MOTION:** S. Lawlor **MOVED** to approve the Ed/Tech Goals as presented. **SECOND:** B. Tatro. **VOTE:** 9.863/0/0/3.137. **Motion passes.** L.Steadman would like to edit Charter #3. The tech plan is maintained by the staff. She would like to delete "maintain". S.Peters explained any changes can be done at the committee level.

8. SETTING NEXT MEETING'S AGENDA:

a. RSVP Graduation
b. Non-Meeting
c. Policy Goals and Charter
d. Fin/Fac. Goals and Charter
e. Superintendent Performance Evaluation
f. Non-Certified Staff pay increase
g. Authorize Manifest Signatures
h. Encumbrance (if any)
i. Completed May 16, 2023 Joint Meeting Agenda

The Board asked if there are still Senior Project Presentations to attend. J. Rathbun explained some of the Senior Projects are electives. There are reasons why it is not a Senior requirement such as scheduling and staffing.

9. **Public Comments:** There were no Public Comments.

10. **8:58 PM: Motion to Enter into Non-Public Session under RSA 91-A:3, II (b) The hiring of any person as a public employee: MOTION:** L. Steadman **MOVED** to enter into Non-Public Session under RSA 91-A:3, II (b) The hiring of any person as a public employee. **SECOND:** K. Noonan **VOTE:** 9.863/0/0/3.317. **Motion passes.**

11. **9:02 PM: Motion to Enter into Non-Public Session under RSA 91-A:3, II (c) Matters which, if discussed in public, would likely adversely affect the reputation of any person, other than a member of the public body itself, unless such person requests an open meeting: MOTION:** K. Noonan **MOVED** to enter into Non-Public Session under RSA 91-A:3,II (c) Matters which, if discussed in public, would likely adversely affect the reputation of any person, other than a member of the public body itself, unless such person requests an open meeting. **SECOND:** B. Tatro. **VOTE:** 9.863/0/0/3.137. **Motion passes.**

12. **9:16 PM: Motion to Enter into Non-Public Session under RSA 91-A:3, II (i) Consideration of matters relating to the preparation for and the carrying out of emergency functions: MOTION:** L.Steadman **MOVED** to enter into Non-Public Session under RSA 91-A:3, II (i) Consideration of matters relating to the preparation for and the carrying out of emergency functions. **SECOND:** K. Noonan **VOTE:** 9.863/0/0/3.317. **Motion passes.**

13. **ADJOURNMENT: MOTION:** K. Noonan **MOVED** to adjourn the meeting at 9:34 PM. **SECOND:** B. Tatro **VOTE:** 9.863/0/0/3.317. **Motion passes.**

Respectfully submitted,

Laura L. Aivaliotis
Recording Secretary

VOTING KEY: Yes/No/Abstain/Absent

Monadnock Regional School District
School Board Meeting Minutes
Non-Public Session (Not Yet Approved)
May 2, 2023
MRMHS Library/Zoom, Swanzey, NH

Members Present: Kristen Noonan, Edmond LaPlante, Scott Peters, Eric Stanley, Betty Tatro, Lisa Steadman, Brian Bohannon via Zoom, Dan LeClair and Stephanie Lawlor. **Absent:** Jennifer Strimbeck, Jeff Cesaitis, Cheryl McDaniel-Thomas and Nick Mosher

Administration Present: J. Rathbun, Assistant Superintendent and J. Morin, Business Administrator.

8:58 PM Non-Public Session RSA 91-A:3 II (b) The hiring of any person as a public employee:

Issue #1: MOTION: K. Noonan **MOVED** to accept the nomination of Rachel Gantt as the grade 5/6 teacher at Emerson and Mackenzie Rokes as the School Counselor at MTC as presented by the administration. **SECOND:** B. Tatro. **VOTE:** 9.863/0/0/3.317. **Motion passes.**

MOTION: K. Noonan **MOVED** to leave Non-Public Session. **SECOND:** B. Tatro **VOTE:** 9.863/0/0/3.3137. **Motion passes.**

Respectfully submitted,

Laura L. Aivaliotis
Recording Secretary

Monadnock Regional School District
School Board Meeting Minutes
Non-Public Session
May 2, 2023
MRMHS Library/Zoom, Swanzey, NH

Members Present: Kristen Noonan, Scott Peters, Eric Stanley, Lisa Steadman, Betty Tatro, Dan LeClair, Brian Bohannon via Zoom, Edmond LaPlante and Stephanie Lawlor. **Absent:** Jennifer Strimbeck, Jeff Cesaitis, Cheryl McDaniel-Thomas, and Nick Mosher.

Administration Present: J. Rathbun, Assistant Superintendent and J. Morin, Business Administrator.

9:02 PM Non-Public Session RSA 91-A:3 II (c) Matters which, if discussed in public, would likely adversely affect the reputation of any person, other than a member of the public body itself, unless such person requests an open meeting.

Issue # 1: MOTION: K. Noonan **MOVED** to approve the 5 intermittent unpaid leave days as presented by the administration. **SECOND:** S. Lawlor **VOTE:** 9.836/0/0/3.137. **Motion passes.**

Issue #2: Notification: The administration notified the Board of the resignation of Mary Swain and Chance Margheim.

Issue #3: Superintendent Performance Evaluation: S.Peters presented the results of the Superintendent Performance Evaluation to the Board. He explained that 8 out of the 13 Board Members participated. He will share the results with L. Witte. S. Lawlor asked if the staff is able to fill out the evaluation and contribute. S. Peters said not this document but one could be created. J. Rathbun would caution you might not want a response to break up a team. S.Peters mentioned a round table feedback discussion.

MOTION: K. Noonan **MOVED** to leave Non-Public Session. **SECOND:** S. Lawlor **VOTE:** 9.863/0/0/3.137. **Motion passes.**

Respectfully submitted,

Laura L. Aivaliotis
Recording Secretary

Monadnock Regional School District
School Board Meeting Minutes
Non-Public Session (Not Yet Approved)
May 2, 2023
MRMHS Library/Zoom, Swanzey, NH

Members Present: Kristen Noonan, Edmond LaPlante, Scott Peters, Eric Stanley, Betty Tatro, Lisa Steadman, Brian Bohannon via Zoom, Dan LeClair and Stephanie Lawlor.
Absent: Jennifer Strimbeck, Jeff Cesaitis, Cheryl McDaniel-Thomas and Nick Mosher

Administration Present: J. Rathbun, Assistant Superintendent and J. Morin, Business Administrator.

9:16 PM Non-Public Session RSA 91-A:3 II (i) Consideration of matters relating to the preparation for the carrying out of emergency functions.

Issue #1: The Board discussed Safety Drills with the administration.

MOTION: K. Noonan **MOVED** to leave Non-Public Session. **SECOND:** B. Tatro
VOTE: 9.863/0/0/3.3137. **Motion passes.**

Respectfully submitted,

Laura L. Aivaliotis
Recording Secretary

Monadnock Regional School District (MRSD)
Joint Meeting of the School Board and the Budget Committee
May 16, 2023 (Not Yet Approved)
MRMHS Library/Zoom, Swanzey, NH

Members Present: Kristen Noonan, Scott Peters, Eric Stanley, Jeff Cesaitis, Dan LeClair, Betty Tatro, Lisa Steadman and Edmond LaPlante. **Absent:** Brian Bohannon, Stephanie Lawlor, Cheryl McDaniel-Thomas, Nick Mosher and Jennifer Strimbeck.

Budget Committee Members: Jon Hoden, Adam Hopkins, Dan Coffman, Ann Marie Osheyack, Robert Audette, Betty Tatro, School Board Liaison and Robert Young. **Absent:** Nancy Carney, Edward Sheldon, Wayne Lechlider, Richie HKS Thackston, Douglas Bersaw and Unassigned Seats from Roxbury and Gilsum.

Administration Present: L. Walker, Superintendent, J. Rathbun, Assistant Superintendent and J. Morin, Business Administrator.

1. **CALL THE MEETING TO ORDER:** S.Peters called the meeting to order at 7:00 PM.
2. **PUBLIC COMMENTS:** There were no public comments.

3. **#CelebrateMRSD:** S. Peters welcomed everyone to the meeting.

a. L. Walker mentioned the many activities that are being done in the district. The students are going to Boston, The Freedom Trail, attend a court trial, plant pumpkins, visit the Friendly Farm, participate in NHDI and ice cream socials to name a few. Gilsum students did a walk challenge in which the whole school walked what is equal to NH 3 times.

b. The Milestone/Award Ceremony was held at Pappagallos.

c. The staff received stainless steel water bottles for Staff Appreciation.

d. Graduation is June 3, 2023 at 10:00 AM. If the Board would like to attend contact L.Sutton.

e. L. Walker had attended and updated the Board and Budget Committee on the School Funding Suit. She explained that there are 18 districts in the Suit. She had testified last week. She said it was interesting and a learning experience. She mentioned that Special Ed. is not part of the Suit.

4. **MATTERS FOR JOINT MEETING INFORMATION & DISCUSSION:**

a. **Superintendent Search:** S. Peters explained that L. Walker will be leaving the district at the end of June 2024. The Board will conduct a search for a new superintendent. The Board has received 2 statements of work, one from the NHSBA and one from NESDEC which we will discuss at the June meeting. An advisory committee has been established. They will define requirements.

b. Specialist Contract Overview: The Budget Committee was provided with the current Specialist Contract. L. Walker reviewed the contract. There are 10 members in the Union. They work 188 days a year, 7 ½ hours a day and have a 25-minute lunch. There are wellness days and staff development. L. Walker explained the insurance and the retirement benefits. This is informational only.

c. Renovation Project Update: J. Morin explained that the 700s and 800s renovations will begin the day after school gets out. A moving company will be helping to remove the contents of the rooms. Hutter Construction is ready to go with the project. The repair of the roof at the MRMHS will be done over the summer. Melanson Roofing will be doing the project. She explained that there are funds for the engineering and design for the Elementary School Renovations. We will be moving ahead with the conversation about the softball field moving and the septic project at MTC. J. Rathbun explained he has been working with K. Barker, T. Cote and L.Spencer about where to put the softball field. It was suggested to put the softball field on the MRMHS campus. Another idea is to move the field hockey to the MTC site. E. Stanley suggested a turf field to fix all of the problems. It was explained that the turf field will cost $800,000.00 and the new softball field is $400,000.00. J. Morin explained that the softball field needs to get done and seeded. We want to get that work done this summer. J. Hoden would like to deforest the area near the MRMHS campus fields. It would be feasible for all of the teams. The trees are a safety concern. He said that he loves the idea of moving the softball field to the MRMHS campus. J. Morin explained that the district is waiting for the State to announce their budget. If there is no Building Aid we will not move ahead with the project. The Bond application is done and needs to be submitted June 16, 2023 which is likely before the announcement of the Building Aid. She is not sure about the Bond Sale. The District may have to wait until January.

d. Capital Improvement & Warrant Ideas for March 2024: S.Peters is asking for the opinion of the Budget Committee. He said if the district does not get the bond and there is a potential delay on the interest payment should the Board introduce a warrant for work to be done at the high school. There is a CIP list. There are things that need to be done. K. Barker will get the accurate list but he is busy at the moment. There are a few million dollars in open projects. J. Hoden would like the list before a decision. What is the Budget Committee's opinion on the timing of the bond and the opinion on how and when to introduce the backlog? J.Hoden suggested waiting until next year, D. Coffman commented if we put the bond off and there is no payment this may be the right time. If there is no payment in the first year he does not want to wait. K. Noonan commented even if there is no payment on the bond we need to communicate it to the public. J. Hoden commented on the safety needs not must haves. E.Stanley commented on the taxes if you take a year off there will be a bigger drop than an increase the next year. K. Noonan suggested the unallocated funds for the projects. S.Peters said that the backlog today is always revolving. Eventually there will be work to be done at the elementary schools. R. Young likes the idea of an expendable trust. He suggested giving the public a 10-year plan. J. Morin responded to a comment about the district procrastinating on work in the schools. The voters have always supported the maintenance warrant. The State has commended us for the maintenance of the schools. We have done well with what the taxpayers are willing to give us. E. Stanley likes the idea of an expendable trust. S.Peters would appreciate a motion regarding a dollar amount for an expendable trust. There will be a warrant article for the budget and the Specialists Contract so far. D. Coffman commented that we are discussing the CIP and we need to focus on the delivery of education. He does not see it on the agenda. It was commented that the Budget Committee will place surplus and the expendable trust on their next agenda.

e. Education Reporting Overview: A.Hopkins had asked the administration at multiple meetings to give an education report to the Budget Committee. S.Peters said he was not going to ask the administration to give the same report to the Budget Committee that the School Board received. A. Hopkins explained that the RSA states that the administration must provide information when asked by the Budget Committee. J.Rathbun reviewed and discussed the data from the test results that he has provided. He explained the main assessment tools and expectations district wide for each grade level. He mentioned that parents can have their kids opt out of the testing. It is difficult to look at the students over the 2 to 3 years with COVID and different assessments. Look at our kids for 2 years and look at the growth over proficiency. A measure does not tell us if what we are doing is working. Growth models let us see and the proficiency models did not do anything. From April 2021 to April 2022 there was growth and something was working. Proficiency was decent. D. Coffman commented that we did see growth and some of the students were below proficiency. J. Rathbun asked what is the definition of proficiency. Culture of the town and a typical family contribute to high levels of proficiency. D. Coffman would like an executive summary. S. Peters asked for the question and the administration will give feedback. J. Rathbun commented that when the State changes the test, proficiency changes. Proficiency is a lot more than the test. J. Rathbun explained in the Spring the PSAT and the SAT are given. This is a hands-off test by the teacher. Again, the students can opt out of the test with parents' permission. We do not promote this but it is a bit of an issue. The forms are available on the website. We do not hide it. The high school was at 83% because 20 of our students opted out. D. Coffman asked if he had a summary of statistics for the SAT and PSAT. J. Rathbun said that he does have a summary that he presents to the Board. Behavior, absence and opt out are reasons for low results. Our top students opted out and we did poorly in Math.The PSAT is given to the 9th and 10th graders as a way to collect data, get the students comfortable with the test and let them go through the experience. IReady is for K-8. He explained the program. The cost of the program is paid for through the CARES funds. Proficiency is explained and growth is shown on the report. The IReady tool provides good reports and good analysis on what the students need. Not all of the teachers were on board but this is a tool we are using and can see where the students need help. A. Hopkins asked if the curriculum costs of 3-5 years have worked and asked if there were favorable results. L. Walker explained that the administration has provided the data. We cannot correlate test scores. J. Rathbun explained we purchase programs based on the student's needs. A. Hopkins would like a list of the purchased item, if it had results, to which group and the cost. Come and sell us on what you need. L. Walker commented that the Budget Committee and the School Board need to communicate. J. Hoden would like to have a student speak. He needs facts and bullets. People want to hear what we are investing in. J. Rathbun mentioned that we need more social workers and guidance counselors. If it is not safe and comfortable at home the student will not learn. The world is not the same as it was 50 years ago. D. Coffman would like a static summary, boil down the results and what are the corrections. J. Rathbun explained there is a 6-page document. D. Coffman wants a summary. J. Rathbun said it does not work that way. D. Coffman would like him to figure it out. R. Young reviewed the test results on the website and compared them to KHS and the State. Our test scores are not good. L. Walker explained the results are because the parents opt out. K. Noonan commented that it would be helpful for the Budget Committee members to receive the packets and attend the School Board Meetings to get the summarized information, it is public. It was commented that it is hard to attend another meeting but think of the administration. It was suggested for J. Rathbun and the Superintendent attend the Budget Committee Meeting. D.LeClair commented on the hour and a half on this issue. ***D.LeClair leaves the meeting.***

f. Overview of Critical Staffing Shortage: L. Walker reviewed the vacancy list provided. She said there were 36 vacancies last year, 45 vacancies this year because of the number of retirements. We have vacancies filled with contracted services. L. Walker had done a survey with 78 SAUs in the State regarding the number and type of vacancies. She had shared the survey with a Legislative Study Committee. The State revamped the survey but she has not seen the results. She explained that the certified staff are hired first but there are options to hire staff without credentials. The hire is assigned a person and mentor and there are classes to help with their professional development. We are investing in our future. The list for the critical survey is not out. There are 14 staff on an alternative plan and some have finished. J. Rathbun explained if a teacher is moving from one subject to another they are on a plan and are included in the 14 staff. They coordinate to work with the teachers. J. Rathbun explained they are working with KSC for options. We want to go after the young teachers, give them professional development and the mentor program.

5. MATTERS THAT REQUIRE BUDGET COMMITTEE ACTION:

a. April 25, 2023 Minutes: The Budget Committee will approve their minutes at their next meeting.

6. BUDGET COMMITTEE ADJOURNMENT: A. Hopkins adjourned the Budget Committee Meeting at 10:20 PM.

7. MATTERS THAT REQUIRE BOARD ACTION:

a. May 2, 2023 Meeting Minutes: The Board will approve the May 2, 2023 Meeting Minutes at their next meeting.

b. Manifest: MOTION: K. Noonan **MOVED** to approve the manifest in the amount of $1,301,053.66 presented by the administration. **SECOND:** B. Tatro **VOTE:**

7.566/0/0/5.534. **Motion passes.**

c. Budget Transfer: The following transfers as presented by J. Morin: a budget transfer as requested by L.Spencer in the amount of $5,937.00 from the Science Supplies line and the Substitute line to the Replacement Furn/Equip. Line for magnetic whiteboard replacement for 700s/800s wing renovation, a budget transfer as requested by L.Spencer in the amount of $7,637.00 from the Library Para Salary line to the Athletic Equipment line to replace Gym Audio System, a budget transfer as requested by L. Spencer in the amount of $40,000.00 from the Nurse Health Benefits line and the Regular Instruction line to the Technology Equipment line to purchase additional chromebooks and a chromebook cart for MRMHS to ensure students have them when needed for testing and general classroom use and a budget transfer as requested by L. Spencer in the amount of $38,778.00 from the Regular Instruction Retirement line, the B &G Health Insurance line and the Business Studies Textbooks line to the Replacement Furn/Equipment line to purchase replacement furniture for 5 classrooms in the 700s/800s wing renovation. **MOTION:** K. Noonan **MOVED** to approve the budget transfers as presented by J. Morin. **SECOND:** B. Tatro. **VOTE:** 7.566/0/0/5.534. **Motion passes.**

d. Charter & Goals: Finance/Facilities: The Finance/Facilities Committee Charter and Goals were not in the packet.

e. Board Goals: The Board will place this on their next agenda.

f. Superintendent Goals: The Board will place this on their next agenda.

8. Setting Next Meeting's Agenda:

1. **Policy Committee and Fin/Fac Committee Charter and Goals**
2. **Authorize Manifest Signature**
3. **Non-Meeting to collect Board Input for Negotiations**
4. **Encumbrances if any**
5. **Board Member Stipends**
6. **Non-Certified Staff Nominations**
7. **Non-Certified Staff Pay Increases**

9. Public Comments: There were no Public Comments.

10. 10:30 PM: Motion to Enter into Non-Public Session under RSA 91-A:3, II (c) Matters which, if discussed in public, would likely adversely affect the reputation of any person, other than a member of the public body itself, unless such person requests an open meeting: MOTION: K. Noonan **MOVED** to enter into Non-Public Session under RSA 91-A:3,II (c) Matters which, if discussed in public, would likely adversely affect the reputation of any person, other than a member of the public body itself, unless such person requests an open meeting. **SECOND:** B. Tatro. **VOTE:** 7.566/0/0/5.534. **Motion passes.**

11. **10:34 PM: Motion to Enter into Non-Public Session under RSA 91-A:3, II (b) The hiring of any person as a public employee: MOTION:** K. Noonan **MOVED** to enter into Non-Public Session under RSA 91-A:3, II (b) The hiring of any person as a public employee. **SECOND:** J. Cesaitis **VOTE:** 7.566/0/0/5.534. **Motion passes.**

12. **ADJOURNMENT: MOTION:** K. Noonan **MOVED** to adjourn the meeting at 10:37 PM. **SECOND:** J. Cesaitis **VOTE:** 7.566/0/0/5.534. **Motion passes.**

Respectfully submitted,

Laura L. Aivaliotis
Recording Secretary

VOTING KEY: Yes/No/Abstain/Absent

Monadnock Regional School District
School Board Meeting Minutes
Non-Public Session (Not Yet Approved)
May 16, 2023
MRMHS Library/Zoom, Swanzey, NH

Members Present: Kristen Noonan, Eric Stanley, Jeff Cesaitis, Betty Tatro, Lisa Steadman, Scott Peters and Edmond LaPlante **Absent:** Jennifer Strimbeck, Brian Bohannon, C. McDaniel-Thomas, Stephanie Lawlor, Dan LeClair and Nick Mosher

Administration Present: L. Walker, Superintendent, J. Rathbun, Assistant Superintendent and J. Morin, Business Administrator.

10:34 PM Non-Public Session RSA 91-A:3 II (b) The hiring of any person as a public employee:

Issue #1: Nomination: MOTION: K. Noonan **MOVED** to accept the nomination of Sara Stewart as presented by the Superintendent. **SECOND:** B. Tatro **VOTE:** 7.566/0//0/5.534. **Motion passes.**

MOTION: K. Noonan **MOVED** to leave Non-Public Session. **SECOND:** J.Cesaitis **VOTE:** 7.566/0/0/5.534. **Motion passes.**

Respectfully submitted,

Laura L. Aivaliotis
Recording Secretary

Monadnock Regional School District
School Board Meeting Minutes
Non-Public Session (Not Yet Approved)
May 16, 2023
MRMHS Library/Zoom, Swanzey, NH

Members Present: Kristen Noonan, Eric Stanley, Jeff Cesaitis, Betty Tatro, Lisa Steadman, Scott Peters, and Edmond LaPlante **Absent:** Jennifer Strimbeck, Brian Bohannon, Dan LeClair, C. McDaniel-Thomas, Stephanie Lawlor and Nick Mosher

Administration Present: L. Walker, Superintendent, J. Rathbun, Assistant Superintendent and J. Morin, Business Administrator.

10:30 PM Non-Public Session RSA 91-A:3 II (c) Matters which, if discussed in public, would likely adversely affect the reputation of any person, other than a member of the public body itself, unless such person requests an open meeting:

Issue #1: Retirement: MOTION: K. Noonan **MOVED** to accept the retirement of Lisa Fisk on June 30, 2024. **SECOND:** J. Cesaitis. **VOTE:** 7.566/0//0/5.534. **Motion passes.**

Issue #2: Rescind Retirement: MOTION: K. Noonan **MOVED** to approve the request to rescind the retirement of Floyd Willis. **SECOND:** J. Cesaitis. **VOTE:** 7.566/0/0/5.534. **Motion passes.**

MOTION: K. Noonan **MOVED** to leave Non-Public Session. **SECOND:** J.Cesaitis **VOTE:** 7.566/0/0/5.534. **Motion passes.**

Respectfully submitted,

Laura L. Aivaliotis
Recording Secretary

Monadnock Regional School District
Finance/Facilities Committee Charter

Board Last Approved: 5/05/2020

The purpose of the Finance/Facilities Committee is to develop and support the following initiatives:

1. Document and refresh (annually) a long-term facilities plan that encompasses all buildings within the district. The plan includes strategies and timelines for both the funding and work effort of all significant projects related to the district's buildings and grounds, as well as strategic purchases such as land, equipment, or consulting services.

2. Work with Administration and the district's consultants (e.g. architects) in developing plans and proposals for projects; present recommendations to the full board

3. Monitor and recommend state/federal/grant funding options as they become available to support the district's project goals; present opportunities and recommendations to the full board

4. Continuously review and draft changes to policy books D (Fiscal Management) and F (Facilities and Planning Development), as well as policies specific to the use of buildings and grounds, and forward those drafts as recommendations to the Policy Committee

5. To hear and review requests from the Administration, Students, Employees, and general public related to proposals for the district's buildings, grounds, and equipment

Last reviewed by committee: 4/12/2022

Finance/Facilities Committee Goals for 2023/24

Board Approved mm/dd/yyyy

1. Ongoing through the year: Monitor the progress of the Elementary Renovations project. Review options presented by the Construction and Architectural firms, and make recommendations to the full board as needed

2. By September 30th: Update the capital improvement plan in both timeline and written format

3. By October 31st: Present the documented plan to the Budget Committee for consideration. This presentation is separate from the annual joint meeting of the Budget Committee and full School Board

4. Optional as time allows: Review the Book D and F policies assigned by the Policy committee and provide recommendations