



Education: Data Security

Section: Education	Effective Date: 08/29/2024
Department: All	Revision Date:
References: Education Law sections 2-d, 101, 207, and 305	
Number of Pages:	Approved: <i>C. Mariano, CEO</i>

Policy

Mountain Lake Academy will ensure that parents, legal guardians, and eligible students (students who are age 18 or older) are afforded all the protections, where applicable, under the Family Education Rights Privacy Act (FERPA) and the Individuals with Disabilities Act (IDEA) and federal regulations.

Procedure

Mountain Lake Academy will align with the National Institute for Standards & Technology (NIST) Cybersecurity Framework to safeguard the confidentiality of data.

Practice

Data Privacy

- The School Principal is responsible for ensuring that the information, programs, and data are secured and protected from unauthorized access, alteration, damage, or accessed by unauthorized persons.
- All data containing confidential or restricted information will be protected in accordance with SED standards and in accordance with applicable laws and regulations.
- Safeguards will be implemented to prevent unauthorized disclosure of data and detect changes to data during transmission.
- All Mountain Lake Academy laptop computers will be secured in accordance with SED Standards.
- Removable media will not be used to store confidential or restricted information.
- Personally identifiable information will only be disclosed to third parties with a written acknowledgement to protect the identifiable information.
- Parents/legal guardians will be notified in accordance with applicable laws and regulations if a breach or unauthorized release of a student's Personally Identified Information occurs.

Risk Management

- Mountain Lake Academy will identify risks to the confidentiality, integrity, and accessibility of data and manage operations and actions of employees to minimize or eliminate identified risk congruent with applicable laws, rules and regulations, and industry recommended practices to include the following:
 - Conduct routine tests to identify vulnerabilities.
 - A contracting process that includes terms and provisions to address the risks to systems and data.
 - Risks to data are identified, assessed, and responded to in an efficient and timely manner.
 - A process to ensure that the protection of data is reviewed for improvements and updates/changes in regulations annually
 - The risk management strategy will be implemented consistently, be periodically reviewed, and updated as required to address academy changes.

Software and Applications

- Detailed information about the software will be documented and provided as needed. The software/application will be updated as recommended using an automated process whenever possible.

Access Control

- Access controls will be implemented to protect against unauthorized alteration, loss, denial, or disclosure of data.
- Access privileges will be granted in accordance with the user's job responsibilities and will be limited only to those necessary to accomplish assigned tasks.
- All employees with access to student data and/or information will complete data privacy and security awareness training on an annual basis.

Data Security

- Data security and data privacy controls will be incorporated into all aspects of the academy's information system.
- Proposed system changes will be reviewed and approved by the Principal prior to implementation.
- Controls will be implemented to ensure the protection of data and systems.

Incident Response Planning and Vulnerability Management

- Mountain Lake Academy has an Emergency Response Plan in the event that there is a need to respond to a data or cybersecurity incident. The Incident Response Plan will be
 - Reviewed annually and updated to address system/organization changes
 - Communicated to staff with incident response responsibilities
 - Protected from unauthorized disclosure or modification.

Repairs and Maintenance

- Repairs and maintenance on all hardware and software will be controlled and performed only by approved personnel. Questions about approval will be addressed by the Academy Principal. Security will be implemented to protect data and information systems from unauthorized access or modification.
 - All maintenance activities will be approved and monitored by designated system/facility staff.
 - To the extent possible, all maintenance activities will be scheduled in advance and approval granted by the impacted parties.
 - All software patches and updates will only be used after research and testing has been conducted.
 - All systems are reviewed on a regular basis to ensure that current practices are applied.
 - Maintenance tools will be inspected, approved, controlled, and monitored.
 - All media will be checked for malicious code before being introduced.
 - A process for maintenance personnel authorization is established and a list of authorized maintenance organization/personnel is maintained.
 - Session and network connections for remote maintenance will be terminated when non-local maintenance is completed.
 - Remote maintenance and diagnostic sessions will be audited, and the records reviewed by designated system/facility staff.

Media Protection

- All information system media (e.g., disk drives, diskettes, internal and external hard drives, portable devices, etc.), including backup media, removable media, and media containing SED information and/or sensitive information will be secured and protected from unauthorized access at all times.

Least Functionality

- Mountain Lake Academy's IT systems will be configured to provide only essential capabilities
- Servers will not be used as workstations.
- The use of high-risk functions will be prohibited or restricted, as appropriate

Accessing a list of Student Data Elements

- A complete list of all student data elements collected by NYSED is available at <https://www.nysed.gov/data-privacy-security/student-data-inventory> and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.

Complaints

- Complaints concerning possible breaches or unauthorized disclosures should be directed to:
Christopher Mariano
Principal
Mountain Lake Academy
386 River Road
Lake Placid, NY 12946
- Complaints concerning possible breaches or unauthorized disclosures may also be submitted to NYSED at <https://www.nysed.gov/data-privacysecurity/parents-and-students-file-privacy-complaint>, by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email to privacy@nysed.gov; or by telephone at 518-474- 0937.