METROPOLITAN LEARNING INSTITUTE

Licensed by the New York State Education Department
Non–Profit Educational Organization
" Innovative Approach Is Our Way to Success "
www.gettraining.org

<table>
<tr><td>

Main Campus:
97-77 Queens Blvd., 9th Floor
Rego Park, NY 11374
Phone (718) 897-0482
Fax (718) 897-5667

</td><td>

Extension:
550 59th Street
Brooklyn, NY 11220
Phone (718) 492-2120
Fax (718) 492-2197

</td></tr>
</table>

MLI Policy on Safeguarding Student Information:

Postsecondary educational institutions participating in the FSA programs are subject to the information security requirements established by the Federal Trade Commission (FTC) for financial institutions.

Student information that must be safeguarded

These requirements apply to all student information in Metropolitan Learning Institute's possession, regardless of whether such information pertains to students, family, or other individuals with whom MLI has a student relationship, or pertains to the students of other financial institutions that have provided such information to MLI. Student information means any record containing nonpublic personal information (see definition) about a student of a given institution, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of MLI or its affiliates.

- *Definition of "nonpublic personal information": Personally identifiable financial information; and any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available.*

All students' nonpublic personal information (personally identifiable financial information, and any list, description, or other grouping of consumers that is derived using any personally identifiable financial information that is not publicly available) whether in paper, electronic or other form, that is handled or maintained by or on behalf of the school or your affiliates, is protected by an information security program.

- All paper records with any identifiable information are shredded when discarded.
- All paper records may be handled only by appropriate department staff and are never left unattended.
- All computers are password protected with a separate password when accessing student information.
- All information from ECM, MLI's third-party servicer, is placed on their FTP site which requires password access.

- All employees are trained, when hired, on the importance of information security and computers are set up with a time constraint (if a computer is not used within a 5 minute timeframe, the computer automatically saves current information and turns off.)
- The software used guarantees information protection as long as the software is used as directed.
- The security system is tested and monitored for any security problems.
- The sharing of COD/NSLDS User IDs and passwords is strictly prohibited.
- The sharing of a student's PIN number is strictly prohibited.

In addition to the above requirements, MLI's information security program includes the following elements:

Designated coordinators: MLI designates an employee or employees to coordinate its information security program.

Risk assessment: MLI identifies reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information and assess the sufficiency of any safeguards in place to control these risks.

MLI's risk assessment includes consideration of risks in each relevant area of its operations, including: • Employee training and management, • Information systems, including network and software design, as well as information processing, storage, transmission, and disposal, and • Detecting, preventing, and responding to attacks, intrusions, or other systems failures.

Safeguards & testing/monitoring: MLI designs and implements information safeguards to control the risks it identifies through risk assessment, and regularly tests or otherwise monitors the effectiveness of the safeguard's key controls, systems, and procedures.

Evaluation & adjustment: MLI evaluates and adjusts its information security program in light of the results of the required testing and monitoring, as well as for any material changes to operations or business arrangements or any other circumstances that it has reason to know may have a material impact on the school's information security program.

Overseeing service providers: A service provider is any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to MLI. MLI takes reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue and requires its service providers by contract to implement and maintain such safeguards.