

NYLC Privacy Policy

Our company has many more assets than you see at your physical location in the school. These assets are information, which is critical to doing business, keeping the trust of our students, keeping the trust of our agency partners and keeping our company strong. This policy outlines our commitment to our employees, students, other customers, and stakeholders regarding how we will handle information. Information can be sensitive by nature, and can also be sensitive due to regulations and industry standards. The types of sensitive information can include:

- Customer (student) information
 - Financial information, including credit cards, salaries, banking, transactions and more
- Medical information of all types
- Company intellectual property
- Company business records and materials, including our student data base, marketing and sales efforts, and more.
- Copyrighted materials, both which our company creates and those which we obtain under license from others.

This information may reside on our computers or backup devices, may travel on our networks, be on paper, or be in people's minds. The rules by which information is handled are determined by the regulations, business requirements, and company commitments relating to that type of information. Put together, these are called the *significance* of the information. Every employee, vendor, contractor, supplier or, agent or representative of our company must be aware of the significance of the information being handled, and ensure that proper controls are applied to prevent copying, disclosure, or other misuse of the information. This Privacy Policy is a part of the overall security and privacy effort of our company.

Penalties for violating these policies may include disciplinary actions up to termination of employment, or termination of the business relationship with our company. Our company relies upon employees and business partners to properly develop, maintain, and operate our systems, networks, and processes which keep our sensitive information safe and properly used. This means that every person and organization handling our information has the responsibility to keep the information safe, no matter where the information is located. This includes computing systems, networks, paper copies, files, business processes, and verbal transmission of information.

We will meet all applicable requirements in properly protecting information, including:

- Laws
- Regulations
- Industry standards
- Contractual commitments



The protections we apply to information assets will be in proportion to the value and sensitivity of the information, and will balance the sensitivity of the information against:

- The cost of controls
- The impact of the controls on the effectiveness of business operations
- The risks of disclosure, modification, destruction, or unauthorized use of the
- Information

We will protect all types of sensitive information, including but not limited to:

- Medical
- Financial
- Credit
- Business transactions
- Personal information, both of our employees and of our students

We will ensure that all personnel at all levels are aware of, and are held accountable for safeguarding information assets.

- We will ensure that access to information is controlled, and based upon, job function and need-to-know criteria.
- We will maintain proper business continuity and security procedures, including information systems, networks, resources, and business processes.
- We will report any suspected or actual breach of these policies, and will cooperate with investigative agencies.