DATA PRIVACY & SECURITY POLICY

I. Purpose

This policy addresses the International Leadership Charter High School's (International Leadership's) responsibility to adopt appropriate administrative, technical and physical safeguards and controls to protect and maintain the confidentiality, integrity and availability of its data, data systems and information technology resources.

II. Policy Statement

It is the responsibility of International Leadership:

(1) to comply with legal and regulatory requirements governing the collection, retention, dissemination, protection, and destruction of information;
(2) to protect personally identifiable information, and sensitive and confidential information from unauthorized use or disclosure;
(3) to address the adherence of its vendors with federal, state and International Leadership requirements in its vendor agreements; and
(4) to communicate its required data security and privacy responsibilities to its users, and train its users to share a measure of responsibility for protecting International Leadership's data and data systems.

III. Standard

International Leadership will utilize the National Institute of Standards and Technology's Cybersecurity Framework v1.1 (NIST CSF or Framework) as the standard for its Data Privacy and Security Program.

IV. Scope

The policy applies to International Leadership employees, interns, volunteers, and consultants, and third-parties who receive or have access to International Leadership's data and/or data systems ("Users").

This policy encompasses all systems, automated and manual, including systems managed or hosted by third parties on behalf of International Leadership and it addresses all information, regardless of the form or format, which is created or used in support of the activities of International Leadership.

This policy shall be published on the International Leadership website and notice of its existence shall be provided to all Users.

V. Oversight

With the help of the school's technology providers, International Leadership's Data Protection Officer shall report any data breaches to the school CEO and summarize any complaints submitted pursuant to Education Law §2-d.

VI. Data Privacy

(1) Laws such as the Family Educational Rights Privacy Act (FERPA), NYS Education Law §2-d and other state or federal laws establish baseline parameters for what is permissible when sharing student PII.

(2) Data protected by law must only be used in accordance with law and regulation and International Leadership policies to ensure it is protected from unauthorized use and/or disclosure.

(3) No student data shall be shared with third parties without a written agreement that complies with state and federal laws and regulations. No student data will be provided to third parties unless it is permitted by state and federal laws and regulations. Third-party contracts must include provisions required by state and federal laws and regulation.

(4) The identity of all individuals requesting personally identifiable information, even where they claim to be a parent or eligible student or the data subject, must be authenticated in accordance with International Leadership procedures.

(5) It is International Leadership's policy to provide all protections afforded to parents and persons in parental relationships, or students where applicable, required under the Family Educational Rights and Privacy Act, the Individuals with Disabilities Education Act, and the federal regulations implementing such statutes. Therefore, International Leadership shall ensure that its contracts require that the confidentiality of student data or teacher or principal APPR data be maintained in accordance with federal and state law and this policy.

(6) Contracts with third parties that will receive or have access to personally identifiable information must include a Data Privacy and Security Plan that outlines how the contractor

will ensure the confidentiality of data is maintained in accordance with state and federal laws and regulations and this policy.

VII. Incident Response and Notification

The school will respond to data privacy and security incidents in accordance with its Incident Response Policy**.** The incident response process will determine if there is a breach. All breaches must be reported to the Data Protection Officer. For purposes of this policy, a breach means the unauthorized acquisition, access, use, or disclosure of student, teacher or principal PII as defined by Education law §2-d, or any International Leadership sensitive or confidential data or a data system that stores that data, by or to a person not authorized to acquire, access, use, or receive the data.

International Leadership will comply with legal requirements that pertain to the notification of individuals affected by a breach or unauthorized disclosure of personally identifiable information.

VIII. Training

International Leadership Users must annually complete International Leadership's information privacy and security training.