Tiegerman
DATA PRIVACY AND SECURITY POLICY

To comply with applicable requirements of New York State Education Law §2-d and the accompanying regulations (collectively, the "NYSED Data Privacy and Security Law"), Tiegerman (the "School") has adopted this Data Privacy and Security Policy (the "Policy"). Unless otherwise indicated, capitalized terms in the Policy have the meanings set forth in the NYSED Data Privacy and Security Law.

Pursuant to the Policy:

- The School has designated a Data Protection Officer with responsibility for implementing the policies and procedures required by the NYSED Data Privacy and Security Law, and to serve as the point of contact for data privacy and security for the School. The School's Data Protection Officer shall annually report to its Chief Operating Officer, Chief Compliance Officer, and Board of Directors on data privacy and security activities, the number and disposition ofreported Breaches or Unauthorized Releases, if any, and a summaiy of any complaints submitted pursuant to Education Law §2-d.
- The School does not sell any Personally Identifiable Information ("PII"), nor does it use or disclose such information for any Commercial or Marketing Purpose or facilitate its use or disclosure by any other party for any Commercial or Marketing Purpose or permit another party to do so
- The School takes appropriate steps to minimize its collection, processing, and transmission of PII.
- The School ensures that it includes provisions in its contracts with third-party contractors, or in separate data sharing confidentiality agreements, that require such third-party contractors to maintain the confidentiality of any student, teacher, and/or principal data they receive from or on behalf of the School in accordance with federal and state law and this Policy.
- The School publishes on its website a parents bill of rights for data privacy and security (the "Bill of Rights") that complies with the provisions ofNYSED Data Privacy and Security Law.
- The School includes the Bill of Rights in every contract it enters into with a third-party contractor that processes PII on its behalf, along with the following supplemental information required by the NYSED Data Privacy and Security Law:
    - the exclusive purposes for which the student data or teacher or principal data will be used by the third-party contractor, as defined in the contract;

- how the third-party contractor will ensure that its subcontractors, or other authorized persons or entities to whom the third-party contractor will disclose the student data or teacher or principal data, if any, will abide by all applicable data protection and security requirements, incluiling but not limited to those outlined in applicable state and federal laws and regulations (e.g., FERPA; Education Law §2-d);
- the duration of the contract, including the contract's expiration date and a description of what will happen to the student data or teacher or principal data upon expiration of the contract or other written agreement (e.g., whether, when, and in what format it will be returned to the educational agency, and/or whether, when, and how the data will be destroyed);
- if and how a parent, student, eligible student, teacher or principal may challenge the accuracy of the student data or teacher or principal data that is collected;
- where the student data or teacher or principal data will be stored, described in such a manner as to protect data security, and the security protections taken to ensure such data will be protected and data security and privacy risks mitigated; and
- how the data will be protected using encryption while in motion and at rest.

The School publishes the foregoing supplemental information on its website.

- The School established and communicates to parents, eligible students, teachers, principals or other staff the School's procedure for filing complaints about Breaches or Unauthorized Releases of student, teacher, or principal data.
- The School safeguards data in accordance with the National Institute for Standards and Technology Framework for Improving Critical Infrastrncture Cybersecurity Version 1. 1.
- Every use and disclosure of PII by the School benefits students and the School (e.g., improving academic achievement, empowering parents and students with information, and/or advancing efficient and effective school operations).
- The School does not include PII in public reports or other documents.
- The School ensures that it affords to parents or eligible students all applicable protections under FERP A and the Individuals with Disabilities Education Act (20 U.S.C. 1400 et seq.), as well as the accompanying regulations.

- The School ensures that its contracts with third•party contractors include the third.party contractors' data security and privacy plans, which must be accepted by the School and must comply with the requirements set forth in the NYSED Data Privacy and Security Law.
- The School annually provides data privacy and security awareness training to its officers and employees with access to PIT. This training includes, without limitation, training on state and federal laws that protect PIT, and how employees can comply with such laws.

- The School will report every discovery or report of a Breach or Unauthorized Release of student, teacher or principal data, including those reported to the School by its third•party contractors, to the New York State Education Department's Chief Privacy Officer without unreasonable delay, but no later than IO calendar days after such discovery or receipt of report.
- The School will notify affected parents, eligible students, teachers and/or principals in the most expedient way possible and without unreasonable delay, but no later than 60 calendar days afterits discove1y of a Breach or Unauthorized Release, or its receipt of a notification of a Breach or Unauthorized Release from a third party contractor, unless that notification would interfere with an ongoing investigation by law enforcement or cause further disclosure of PII by disclosing an unfixed security vulnerability.
- The School will ensure that the notifications it provides in the event of a Breach or Unauthorized Release are clear, concise, use language that is plain and easy to understand, and, to the extent available, include: a brief description of the Breach or Unauthorized Release; the dates of the incident and the date of discovery, if known; a description of the types of PIT affected; an estimate of the number of records affected; a brief description of the School's investigation or plan to investigate; and contact infonnation for representatives who can assist parents or eligible students that have additional questions.
- Parents and eligible students have the right to inspect and review a student's education record maintained by the School. All requests to inspect and review must be made by au individual or their representative in writing to the School in accordance with the School's access request procedure. The School will notify parents annually of their right to request to inspect and review their child's education record including any student data stored or maintained by the School.

4857-5742-0433, v. 1