5676 PRIVACY AND SECURITY FOR STUDENT DATA AND TEACHER AND PRINCIPAL DATA

Finn Academy follows all applicable laws and regulations for the handling and storage of student data and teacher and principal data in the School and when disclosing or releasing it to others, including, but not limited to, third-party contractors. The School adopts this policy to implement the requirements of Education Law Section 2-d and its implementing regulations, and to align the School's data privacy and security practices with the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1).

Data Collection Transparency and Restrictions

The School will take steps to minimize its collection, processing, and transmission of PII. Additionally, the School will:

a. Not sell PII nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.
b. Ensure that it has provisions in its contracts with third-party contractors or in separate data sharing and confidentiality agreements that require the confidentiality of shared student data or teacher or principal data be maintained in accordance with law, regulation, and School policy.

Except as required by law or in the case of educational enrollment data, the School will not report to NYSED the following student data elements: juvenile delinquency records; criminal records; medical and health records; and student biometric information.

Nothing in Education Law Section 2-d or this policy should be construed as limiting the administrative use of student data or teacher or principal data by a person acting exclusively in the person's capacity as an employee of the School.

Chief Privacy Officer

The School will comply with directives of, and report breaches or unauthorized releases of student data or teacher or principal data to, the Chief Privacy Officer appointed by the Commissioner of Education in accordance with Education Law Section 2-d, its implementing regulations, and this policy.

Data Protection Officer

The Board of Trustees shall designate a School employee to serve as the School's Data Protection Officer-responsible for the implementation and oversight of this policy and any

related procedures including those required by Education Law Section 2-d and its implementing regulations, as well as serving as the main point of contact for data privacy and security for the School. Some aspects of this role may be outsourced to a provider such as a BOCES, to the extent available.

School Data Privacy and Security Standards

The School will use the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1) (Framework) as the standard for its data privacy and security program.

The School affords all protections under FERPA and the Individuals with Disabilities Education Act and their implementing regulations to parents or eligible students, where applicable.

Third-Party Contractors

Whenever it enters into a contract or other written agreement with a third-party contractor under which the third-party contractor will receive student data or teacher or principal data from the School, the contract or written agreement will include provisions requiring that confidentiality of shared student data or teacher or principal data be maintained in accordance with law, regulation, and School policy. In addition, the contract or written agreement shall include the third-party contractor's data privacy and security plan that complies with the state requirements and that has been accepted by the School, and such third-party contractors are required to comply with state requirements.

Where a third-party contractor engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on the third-party contractor by law and contract apply to the subcontractor.

Click-Wrap Agreements

Periodically, School staff may wish to use software, applications, or other technologies in which the user must "click" a button or box to agree to certain online terms of service prior to using the software, application, or other technology. These are known as "click-wrap agreements" and are considered legally binding "contracts or other written agreements" under Education Law Section 2-d and its implementing regulations.

School staff are prohibited from using software, applications, or other technologies pursuant to a click-wrap agreement in which the third-party contractor receives student data or teacher or principal data from the School unless they have received prior approval from the School's Data Privacy Officer or designee.

The School will develop and implement procedures requiring prior review and approval for staff use of any software, applications, or other technologies pursuant to click-wrap agreements.

Parents' Bill of Rights for Data Privacy and Security

Finn Academy has published on its website a Parents' Bill of Rights for Data Privacy and Security ("Bill of Rights") that complies with state requirements. The Bill of Rights also includes supplemental information that complies with state requirements for each contract the School enters into with a third-party contractor where the third-party contractor receives student data or teacher or principal data from the School.

The School will publish on its website the supplement to the Bill of Rights (i.e., the supplemental information described above) for any contract or other written agreement it has entered into with a third-party contractor that will receive PII from the School. The Bill of Rights and supplemental information may be redacted to the extent necessary to safeguard the privacy and/or security of the School's data and/or technology infrastructure.

Additionally, the School will include the Bill of Rights with every contract or other written agreement it enters into with a third-party contractor under which the third-party contractor will receive student data or teacher or principal data from the School.

Right of Parents and Eligible Students to Inspect and Review Students' Education Records

Consistent with the obligations of the School under FERPA, parents and eligible students have the right to inspect and review a student's education record by making a request directly to the School in a manner prescribed by the School. Requests by a parent or eligible student for access to a student's education records must be directed to the School and not to a third-party contractor. The School may require that requests to inspect and review education records be made in writing.

Only authorized individuals are able to inspect and review student data. To that end, the School will take steps to verify the identity of parents or eligible students who submit requests to inspect and review an education record and verify the individual's authority to do so.

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 through its annual FERPA notice. A notice separate from the School's annual FERPA notice is not required.

The School will comply with a request for access to records within a reasonable period, but not more than 45 calendar days after receipt of a request.

The School may provide the records to a parent or eligible student electronically if the parent consents. The School must transmit the PII in a way that complies with laws and regulations. Safeguards associated with industry standards and best practices, including but not limited to

encryption and password protection, must be in place when education records requested by a parent or eligible student are electronically transmitted.

Complaints of Breach or Unauthorized Release of Student Data and/or Teacher or Principal Data

The School will inform parents, through its Parents' Bill of Rights for Data Privacy and Security, that they have the right to submit complaints about possible breaches of student data to the Chief Privacy Officer at NYSED. In addition, the School has established procedures for parents, eligible students, teachers, principals, and other School staff to file complaints with the School about breaches or unauthorized releases of student data and/or teacher or principal data that will be disseminated to parents, eligible students, teachers, principals, and other School staff.

The School will maintain a record of all complaints of breaches or unauthorized releases of student data and their disposition in accordance with applicable data retention policies, including the Records Retention and Disposition Schedule ED-1 (1988; rev. 2004).

Reporting a Breach or Unauthorized Release

The School will report every discovery or report of a breach or unauthorized release of student data or teacher or principal data within the School, or notification from a third-party contractor of any unauthorized release of the data by the third-party contractor or its assignee, to the Chief Privacy Officer without unreasonable delay, in compliance with state reporting procedures and requirements.

Notification of a Breach or Unauthorized Release

The School will notify affected parents, eligible students, teachers, and/or principals in the most expedient way possible and without unreasonable delay, but no more than 60 calendar days after the discovery of a breach or unauthorized release of PII by the School or the receipt of a notification of a breach or unauthorized release of PII 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. Where notification is delayed under these circumstances, the School will notify parents, eligible students, teachers, and/or principals within seven calendar days after the security vulnerability has been remedied or the risk of interference with the law enforcement investigation ends.

Notifications will be clear, concise, use language that is plain and easy to understand, and to the extent available, include all information -- and will be provided -- as required by law and regulation.

Annual Data Privacy and Security Training

Finn Academy will annually provide data privacy and security awareness training to its officers and staff with access to PII. This training will include, but not be limited to, training on the applicable laws and regulations that protect PII and how staff can comply with these laws and regulations. The School may deliver this training using online training tools. Additionally, this training may be included as part of the training that the School already offers to its workforce.

Notification of Policy

Finn Academy will publish this policy on its website and provide notice of the policy to all its officers and staff.

Education Law § 2-d
8 NYCRR Part 121