NYCACS PERSONALLY IDENTIFIABLE INFORMATION PROTECTION POLICY

SEPTEMBER, 2020

Policies and Procedures

I. Overview

NYC Autism Charter Schools ("NYCACS" or "School") is required by law to collect and store educator and student information. NYCACS takes seriously its obligations to protect the privacy of data collected, used, shared, and stored by the School. Educational data is essential to NYCACS' mission to ensure that all students are prepared for success in society, work, and life. NYCACS is responsible for activities that require the collection of student data, which include, for example: skill acquisition and behavior reduction data, authorizer accountability, state and federal funding, state and federal assessment requirements, program participation and evaluation, and the fulfillment of state and federal reporting requirements. The School is also responsible for several activities that require the collection of education personnel data including issuing and renewing educator licenses and monitoring implementation of educator evaluation systems.

NYCACS has adopted the policy below to protect educator and student data that is collected, used, shared, and stored by NYCACS.

II. Confidentiality of Student PII

Student Personally Identifiable Information (PII) includes, but is not limited to, information that is collected, maintained, generated, or inferred and that, alone or in combination, personally identifies an individual student or the student's parent(s) or family. PII, as defined by federal law, also includes other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates.

Some examples of PII collected by NYCACS may include, but are not limited to, the following list:

- A student's name
- A personal identifier such as a student ID number
- Other indirect identifiers such as a student's date of birth
- Records regarding a student's primary disability
- A student's socioeconomic information
- Photos, videos, and voice recordings
- Assessment results
- Classroom or group information
- Work internship placement information
- Attendance and mobility information between and within school districts
- Special education data and special education discipline reports
- Program participation information required by state or federal law

Student education records are official and confidential documents protected by the Family Educational Rights and Privacy Act (FERPA), the Student Data Transparency and Security Act, and other state and

federal laws. With the increasing use of technology in education, it is imperative that information that identifies individual students and their families is protected from misappropriation and misuse.

III. Confidentiality of Educator PII

Educator PII includes, but is not limited to: the educator's name, any unique identifier, including social security number, and other information that, alone or in combination, is linked or linkable to a specific educator. All papers filed at NYCACS that contain personal information about holders of educator licenses or authorizations are classified as confidential. The information may be shared in the normal and proper course of business, but it is otherwise unlawful for any NYCACS employee or other person to divulge, or make known in any way, any such personal information without the written consent of the educator.

While NYCACS may collect information concerning an individual educator's performance evaluation ratings, etc., this information must remain confidential and may not be published in any way that would identify the individual educator.

Each educator has the right to inspect and to have copies made (at the educator's expense) of all information pertaining to the educator that is held by NYCACS. Educators may challenge any such record by formal letter or other evidence, which shall be added to NYCACS' records.

IV. Disclosure of De-Identified or Aggregate Data

NYCACS may disclose information that does not allow any individual to be personally identified through the process outlined by NYCACS' aggregate data request process. Data requested via this process will not include counts of less than 16 students or five educators in order to reduce the likelihood that this information is personally identifiable for small populations.

V. External Disclosures of and Access to PII

The School will only release PII to outside entities or individuals that have a legitimate educational purpose to receive this information. NYCACS is authorized to share PII for research purposes, so long as the sharing is permitted by state and federal law.

In compliance with state and federal laws, NYCACS limits access to educator and student PII to the following:

- The authorized staff of the School that require access to perform assigned duties
- The School's contractors that require access to perform assigned or contractual duties as stated in the contract
- School district administrators, teachers, and school personnel who require access to perform assigned duties
- The authorized staff of other state agencies, including public institutions of higher education, as required by law and defined by interagency agreements
- Entities conducting research on behalf of the School to develop, validate, or administer tests, administer financial aid programs or improve instruction, as permitted by law and defined by research data sharing agreements
- Vendors, third parties, and other service providers that provide or service databases, assessments, or instructional supports as permitted by law and defined by contractual agreements

- Authorized representatives of NYCACS in connection with an audit or evaluation of Federal- or State- supported education programs, or for the enforcement of or compliance with Federal legal requirements that relate to those programs.

Students and/or their parents or legal guardians are allowed access to the student's PII and educators are allowed to access their own PII in accordance with state and federal law. NYCACS is authorized to share educator PII for research purposes, so long as the data is collected per established protocol and is used in a manner that protects the identity of the educator.

Educator Data, including an educator's name and contact information (including work office, cell and fax phone numbers, work address, and title) can be shared with outside entities and individuals provided the data is protected using sensible privacy and security controls. If this information includes or is associated with any other data, the disclosure must be for a legitimate educational purpose and must be protected via the appropriate contract or agreement.

A. Disclosures of PII for Research Purposes

NYCACS has developed a process to consider and review all outside requests for PII or individual-level data by individuals who seek to conduct research. Potential users such as doctoral and master's degree candidates, university faculty, independent researchers, and private and public agencies must submit proposals before receiving PII or individual-level data to conduct and publish their research. The requestor must meet all of NYCACS' criteria prior to submitting the proposal for any individual-level deidentified data or PII.

NYCACS will conduct an extensive internal review of the research proposal. Should NYCACS approve the research request, the request will be provided to the State Board of Education for their approval. Once fully approved, NYCACS and the researcher will enter into a research data sharing agreement that includes the requirements listed below. Approval to use the PII or individual-level data for one study, audit, or evaluation does not confer approval to use it for another.

NYCACS has the right to review any data prior to publication and to verify that proper disclosure avoidance techniques have been used. NYCACS also has the right to approve reports prior to publication to ensure they reflect the original intent of the agreement.

B. Requirements for Agreements and Contracts to Disclose PII

Prior to sharing PII, the School must enter into a written agreement or contract that meets the following requirements:

- Designates the individual or entity that will serve as the authorized representative or primary individual responsible to protecting and managing PII;
- Specifies the purpose and scope of the contract or agreement;
- Specifies the duration of the contract or agreement;
- Outlines the types of PII that are collected, used, or maintained under the contract or agreement;
- Describes the uses of PII under the contract or agreement; and
- Specifies the length of time that PII can be held.

In addition to all of the precautions addressed above, any agreement or contract shall also address the following assurances to protect PII from further disclosure and unauthorized use:

- Requires the third party to use PII only to meet the purpose stated in the written agreement and not for further disclosure, unless authorized.
- Requires the entity or individual must have a training program to teach its employees about how to protect PII.
- Affords NYCACS the right to conduct audits or other monitoring activities of the entity or individual's policies, procedures, and systems.
- Affords NYCACS the right to verify that the entity or individual has a comprehensive information security program to protect all PII. This includes requirements stating how to respond to any breach in security, including the requirement that any breach in security must be reported immediately to NYCACS.

Prior to sharing PII for research purposes, the School must enter into a written agreement or contract that meets the requirements outlined above. In addition, the agreements must include the following:

- The research methodology and the rationale for why disclosure of PII is necessary to accomplish the research.
- The requirement that the researcher conduct the study in a manner that does not permit the personal identification of educators or students by anyone other than authorized persons of the authorized organization with legitimate interests.
- The assurance that the researcher will maintain the confidentiality of PII at all stages of the study, including within the final report, by using appropriate disclosure avoidance techniques.
- The requirement that the authorized representative destroy the PII at the conclusion of the research according to a specific time period for destruction stated in the agreement.

C. Consequences for Failure to Comply with Agreements or Contracts

An individual may file a written complaint with NYCACS regarding an alleged violation of an agreement or contract. A complaint must contain specific allegations of fact that give reasonable cause to believe that a violation of a data sharing agreement or contract has occurred. NYCACS will investigate all reasonable and timely complaints. NYCACS may also conduct its own investigation when no complaint has been filed or when a complaint has been withdrawn to determine whether or not a violation has occurred.

Should NYCACS determine that an outside individual or entity has committed a material breach of the contract that results in the misuse or unauthorized release of PII, NYCACS will determine whether to terminate the contract in accordance with a policy adopted by the State Board of Education. At a minimum, the policy must require the State Board to hold a public meeting that includes the discussion of the nature of the material breach. The State Board must determine whether to direct NYCACS to terminate or continue the contract. In addition, NYCACS may deny the individual further access to personally identifiable data for at least five years or NYCACS may pursue penalties permitted under state contract law, such as liquidated damages.

VI. Internal Use of PII

PII is only available to employees who have a reasonable and appropriate educational purpose to receive that information. The School's Data Protection Officer will ensure that PII is properly handled from collection to reporting. This person assists in identifying the NYCACS employees who have a legitimate need for access to PII. This person is also charged with developing policies concerning the management of the School's PII.

VII. Security Practices

NYCACS maintains an information security policy and plan. NYCACS also monitors all access and access attempts to all of its data systems and maintains a centralized authentication and authorization process to further track access and safeguard PII.

VIII. Breaches in Security

Employees and contractors must report any possible incidents or breaches immediately to the School's Data Protection Officer. Incidents include, but are not limited to, (i) successful attempts to gain unauthorized access to a State system or PII regardless of where such information is located; (ii) unwanted disruption or denial of service; (iii) the unauthorized use of a School system for the processing or storage of data; (iv) changes to School system hardware, firmware, or software characteristics without the School's knowledge, instruction, or consent; or (v) a breach in a contract that results in the misuse or unauthorized access to PII.

If the Data Protection Officer determines that one or more employees or contracted partners have substantially failed to comply with the School's information security and privacy policies, they will identify appropriate consequences, which may include termination of employment or a contract as well as further legal action.

Concerns about security breaches that involve the Data Protection Officer must be reported immediately to the School's Board.

IX. Staff Training

In order to minimize the risk of human error and misuse of information, NYCACS provides a range of training for all staff using PII. All new NYCACS employees and contracted partners must sign and obey the NYCACS Employee Acceptable Use Policy, which describes the permissible uses of state technology and PII. New NYCA employees and contracted partners also must sign and obey the NYCACS Confidentiality Agreement, which describes appropriate uses and the safeguarding of PII. Employees are required to participate in an annual information security and privacy fundamentals training, which is mandatory for continued access to the School's network.

X. PII Retention and Disposition

The PII that NYCACS collects is maintained according to the retention and disposition schedules outlined by the New York State. For information defined as "Student Permanent Record" (i.e., demographics, enrollment and academic performance data), NYCACS archives this information and protects it with appropriate technical, physical, and administrative safeguards in accordance with state and federal law.

XI. Process for Maintaining this Policy

NYCACS monitors changes in state and federal regulations that are related to the collection and reporting of PII and updates NYCACS policies and procedures to address any new requirements and best practices.

XII. Questions

Questions about NYCACS' privacy or security practices should be directed to Julie Fisher, Executive Director, at JFisher@nycacharterschool.org.