ICS Data Privacy and Security Policy

I. Purpose

This policy addresses Integration Charter Schools (ICS) 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 ICS: (1) to comply with legal and regulatory requirements governing the collection, retention, dissemination, protection, and destruction of information; (2) to maintain a comprehensive Data Privacy and Security Policy designed to satisfy its statutory and regulatory obligations, enable and assure core services, and fully support the organization's mission; (3) to protect personally identifiable information, and sensitive and confidential information from unauthorized use or disclosure; (4) to address the adherence of its vendors with federal, state and SED(State Education Department) requirements in its vendor agreements; and (5) to communicate its required data security and privacy responsibilities to its users, and train its users to share a measure of responsibility for protecting ICS's data and data systems.

III. Standard

ICS will utilize the US Department of Commerce National Institute of Standards and Technology's Cybersecurity Framework v 1.1 (NIST CSF or Framework) as the standard for its Data Privacy and Security Program.

IV. Scope

The policy applies to ICS employees, interns, volunteers, consultants, and third-parties who receive or have access to ICS'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 ICS and it addresses all information, regardless of the form or format, which is created or used in support of the activities of ICS. This policy shall be published on the ICS website and notice of its existence shall be provided to all Users. The policy relates to the protections of "private information" under State Technology Law §208 and the NY SHIELD Act; and the protections of "personally identifiable information" ("PII") of students, teachers, and principals under Education Law §2-d and Part 121 of the Regulations of the Commissioner of Education. Personally identifiable information is defined on page 4 and includes: 1. social security number; 2. home address or telephone number; 3. personal email address; 4. Internet identification name or password; 5. parent's surname prior to marriage; and 6. drivers' license number .

V. Compliance

The Data Privacy Officer is responsible for the compliance of our policy, related policies, and their applicable standards, guidelines and procedures. Instances of non-compliance will be addressed on a case-by-case basis. All cases will be documented, and managers will be directed to adopt corrective practices, as applicable.

VI. Oversight

ICS's Data Privacy Officer shall annually report to the Board of Directors on data privacy and security activities, the number and disposition of reported breaches, if any, and a summary of any complaints submitted pursuant to Education Law §2-d.

VII. 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 ICS policies to ensure it is protected from unauthorized use and/or disclosure.

(3) ICS will establish a Data Governance Team to manage its use of data protected by law. The Data Governance Team will include, at a minimum, the Data Privacy Officer, the Director of Information Technology, the Director of Operations and the Director of Program Evaluation. The Data Governance Team will, together with senior management, determine whether a proposed use of personally identifiable information would benefit students and educational agencies, and to ensure that personally identifiable information is not included in public reports or other public documents, or otherwise publicly disclosed;

(4) 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.

(5) 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 ICS procedures.

(6) It is ICS'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, ICS shall ensure that its contracts require that the confidentiality of student data or teacher or principal data be maintained in accordance with federal and state law and this policy.

(7) The School will ensure that contracts with third-party contractors or separate data sharing and confidentiality agreements require the confidentiality of shared student and/or teacher

or principal PII be maintained in accordance with federal and state law and the School's data security and privacy policy.

Each third-party contractor that receives student data and/or teacher or principal data must:

1. adopt technologies, safeguards and practices that align with the NIST CSF;
2. comply with the School's data security and privacy policy and applicable laws impacting the School;
3. limit internal access to PII (personal identifiable information) to sub-contractors that need access to provide the contracted services;
4. not use the PII for any purpose not explicitly authorized in its contract;
5. not disclose any PII to any other party without the prior written consent of the parent or eligible student (i.e., students who are eighteen years old or older):

- except for authorized representatives of the third-party contractor to the extent they are carrying out the contract and in compliance with state and federal law, regulations and its contract with the School; or
- unless required by statute or court order and the third-party contractor provides notice of disclosure to the School no later than the time the information is disclosed, unless providing notice of disclosure is expressly prohibited by the statute or court order.

6. maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of PII in its custody;
7. use encryption to protect PII in its custody while in motion or at rest; and
8. not sell, use, or disclose PII 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. Third party contractors may release PII to subcontractors engaged to perform the contractor's obligations, but such subcontractors must abide by data protection obligations of state and federal law, and the contract with the School;

VIII. Third-Party Contractors' Data Security and Privacy Plan

The School will ensure that contracts with all third-party contractors include the third-party contractor's data security and privacy plan. This plan must include a signed copy of the Parents' Bill of Rights and must be accepted by the School. At a minimum, each plan will:

1. outline how the third-party contractor will implement all state, federal, and local data security and privacy contract requirements over the life of the contract, consistent with this policy;
2. specify the administrative, operational and technical safeguards practices it has in place to protect PII it will receive under the contract;
3. demonstrate that it complies with the requirements of Section 121.3(c) of Part 121;
4. specify how officers or employees of the third-party contractor and its assignees who have access to student and/or teacher or principal data receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access;
5. specify if the third-party contractor will utilize sub-contractors and how it will manage those relationships and contracts to ensure PII is protected;
6. specify how the third-party contractor will manage data security and privacy incidents that implicate PII including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the School;

7. describe if, how and when data will be returned to the School, transitioned to a successor contractor, at the School's option and direction, deleted or destroyed by the third-party contractor when the contract is terminated or expires.

IX. Incident Response and Notification

ICS will respond to data privacy and security incidents in accordance with procedures in this policy. The incident response process will determine if there is a breach. All breaches must be reported to the Data Privacy 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 ICS 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.

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

The Data Privacy Officer will report every discovery or report of a breach or unauthorized release of student and/or teacher or principal PII to the State's Chief Privacy Officer without unreasonable delay, but no more than ten calendar days after such discovery. 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 or third- party contractor notification. However, if notification would interfere with an ongoing law enforcement investigation, or cause further disclosure of PII by disclosing an unfixed security vulnerability, the School will notify parents, eligible students, teachers and/or principal within seven calendar days after the security vulnerability has been remedied, or the risk of interference with the law enforcement investigation ends. The President and/or his/her designee, in consultation with the Data Privacy Officer, will establish procedures to provide notification of a breach or unauthorized release of student, teacher or principal PII, and establish and communicate to parents, eligible students, and School staff a process for filing complaints about breaches or unauthorized releases of student, teacher, or principal PII.

"Private information" is defined in State Technology Law §208, and includes certain types of information, outlined in the accompanying regulation, which would put an individual at risk for identity theft or permit access to private accounts. "Private information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records. Any breach of the School's information storage or computerized data which compromises the security, confidentiality, or integrity of "private information" maintained by the School must be promptly reported to the President and the Board of Directors. The Board directs the President, in accordance with appropriate business and technology personnel, to establish policies which:

- Identify and/or define the types of private information that is to be kept secure;
- Include procedures to identify any breaches of security that result in the release of private information; and
- Include procedures to notify persons affected by the security breach as required by law.

Employee "Personal Identifying Information" under Labor Law § 203-d Pursuant to Labor Law §203-d, the School will not communicate employee "personal identifying information" to the general public. This includes: 1. social security number; 2. home address or telephone number; 3. personal email address; 4. Internet identification name or password; 5. parent's surname prior to marriage; and 6. drivers' license number. 6 In addition, the School will protect employee social security numbers in that such numbers will not be: • publicly posted or displayed; • visibly printed on any ID badge, card or time card; • placed in files with

unrestricted access; or • used for occupational licensing purposes. • Employees with access to such information will be notified of these prohibitions and their obligations.

X. Acceptable Use Policy, User Account Password Policy and other Related Department Policies

(1) Users must comply with ICS's Information Security Procedure, which outlines the responsibilities of all users of ICS information systems to maintain the security of the systems and to safeguard the confidentiality of ICS information.

(2) Users must comply with this Policy in using Department resources. Access privileges will be granted in accordance with the user's job responsibilities and will be limited only to those necessary to accomplish assigned tasks in accordance with ICS's mission and business functions.

(3) Users must comply with the User Account Password Policy.

(4) All remote connections must be made through managed points-of-entry in accordance with the Data Privacy and Security Guidelines for Remote Work and Telecommuting.

XI. Training

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