

DATA PRIVACY AND SECURITY POLICY

I. Purpose

This policy addresses Saranac School District'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 Saranac Central School District (SCSD):

- (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 Program designed to satisfy its statutory and regulatory obligations, enable and assure core services, and fully support the District'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 requirements in its vendor agreements;
- (5) to train its users to share a measure of responsibility for protecting SCSD student data and data systems;
- (6) to identify its required data security and privacy responsibilities and goals, integrate them into relevant processes, and commit the appropriate resources towards the implementation of such goals; and
- (7) to communicate its required data security and privacy responsibilities and goals and the consequences of non-compliance, to its users.

III. Standard

SCSD will utilize the 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 SCSD employees, and also to independent contractors, interns, volunteers ("Users") and third-party contractors who receive or have access to SCSD data and/or data systems.

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

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

V. Compliance

The SCSD Board of Education and administration are responsible for the compliance of their programs and offices with this 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 program offices will be directed to adopt corrective practices, as applicable.

VI. Oversight

The SCSD Data Protection Officer shall annually report to its Board of Education on data privacy and security activities and progress, the number and disposition of reported breaches, if any, and a summary of any complaint 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 SED policies to ensure it is protected from unauthorized use and/or disclosure.
- (3) SCSD has established a Data Protection Officer and Administrative Team to manage its use of data protected by law. The Data Protection Officer and the Administrative Team will, together with program offices, 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 SCSD procedures.
- (6) It is SCSD 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, SCSD 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.
- (7) 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.

VIII. Incident Response and Notification

The SCSD will respond to data privacy and security critical incidents in accordance with its **Incident Response Plan**. All breaches of data and/or data systems must be reported to the Data Protection Officer and Administrative Team. All breaches of personally identifiable information or sensitive/confidential data must be reported to the 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 SED 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.

State and federal laws require that affected individuals must be notified when there has been a breach or unauthorized disclosure of personally identifiable information. Upon receiving a report of a breach or unauthorized disclosure, the Data Protection Officer, Administrative Team, and other subject matter experts if applicable will determine whether notification of affected individuals is required, and where required, effect notification in the most expedient way possible and without unreasonable delay.

IX. Acceptable Use Policy, Password Policy and other Related Department Policies

(1) Users must comply with the **Acceptable Use Policy** in using District 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 State Entity missions and business functions (i.e., least privilege). Accounts will be removed, and access will be denied for all those who have left the agency or moved to another department.

X. Training

All users of District data, data systems and data assets must annually complete the information security and privacy training offered by the department. Information security and privacy training will be made available to all users. Employees must complete the training annually.

Adoption Date: June 15, 2020

Saranac Central School District

Parents' Bill of Rights for Data Privacy and Security

The Saranac Central School District is committed to ensuring student privacy in accordance with local, state and federal regulations and District policies. To this end and pursuant to U.S. Department of Education (DOE) regulations (Education Law §2-d), the District is providing the following Parents' Bill of Rights for Data Privacy and Security:

- A student's personally identifiable information cannot be sold or released for any commercial or marketing purposes.
- Parents have the right to inspect and review the complete contents of their child's education record, including any student data maintained by the Saranac Central School District. This right of inspection of records is consistent with the federal Family Educational Rights and Privacy Act (FERPA). Under the more recently adopted regulations (Education Law §2-d), the rights of inspection are extended to include data, meaning parents have the right to inspect or receive copies of any data in their child's educational record.
- State and federal laws protect the confidentiality of personally identifiable information and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls and password protection, must be in place when data is stored or transferred.
- A complete list of all student data elements collected by the state is available for public review in an Excel file at

<http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx>

Parents may also obtain a copy of this list by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, N.Y. 12234.

- Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed to: Steven Grenville, Data Protection Officer. Complaints to SED should be directed to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; the e-mail address is cpo@mail.nysed.gov. Complaints may also be submitted using the form available at the following website: <http://www.nysed.gov/student-data-privacy/form-report-improper-disclosure>.

We _____ (vendor name) agree to abide by Saranac CSD Data and Security Privacy Policy and the Parents' Bill of Rights. The information we've provided in response to the supplemental informational questions is true and correct (see appendix).

Sign _____

Date _____

APPENDIX

Supplemental Information Regarding Third-Party Contractors

In the course of complying with its obligations under the law and providing educational services to District residents, the Saranac Central School District has entered into agreements with certain third-party contractors. Pursuant to these agreements, third-party contractors may have access to "student data" and/or "teacher or principal data," as those terms are defined by law and regulation.

For each contract or other written agreement that the District enters into with a third party contractor where the third-party contractor receives student data or teacher or principal data from the District, the following supplemental information will be included with this Bill of Rights:

- 1) 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;
- 2) How the third-party contractor will ensure that the 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, including but not limited to those outlined in applicable laws and regulations (e.g., FERPA; Education Law Section 2-d);
- 3) 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 District, and/or whether, when, and how the data will be destroyed);
- 4) 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;
- 5) Where the student data or teacher or principal data will be stored, described in a manner as to protect data security, and the security protections taken to ensure the data will be protected and data privacy and security risks mitigated; and
- 6) Address how the data will be protected using encryption while in motion and at rest.