The Summit Center
Policies

POLICY NUMBER & TITLE:	10100 Data Security and Privacy Policy (NYSED 2-d)		
Owner:	CIO & CCPO	**Policy Division:**	Privacy & Security
Effective:	01/05/21	**Last Reviewed/Revised:** (QA/CC Only)	4/22/2021

PURPOSE

This policy addresses The Summit Center'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.

SCOPE

This policy applies to the following:

☒ Employees ☒ Consultants ☒ Vendors
☒ Board of Directors ☒ Contractors ☒ Volunteers

In the following programs/departments:

Early Intervention & Education Division	**Behavioral Health Division**	**Community Division**	**Adult Division**
☒ Academy Preschool Integrated	☐ Behavioral Pediatrics Clinic	☐ B.F.F.S.	☐ ACCES-VR
☒ Academy Preschool Self-Contained	☐ Consulting & Professional Training	☐ Community Habilitation	☐ Community Pre-Vocational
☒ Academy School-age	☐ Pediatric Feeding Clinic	☐ Family Education & Training	☐ P.A.C.E.
☒ DDC Evaluations	☐ Summer Programs	☐ Intensive Behavioral Support	☐ Pathway to Employment
☒ Early Autism Program	☐ Other:	☐ Intensive Respite	☐ SEMP
☒ Eligibility Evaluations		☐ L.A.F.F.S.	☐ S.T.E.P.S (Day Habilitation)
☐ Other:		☐ Respite On-Site	☐ Other:
		☐ Respite Off-Site	
		☐ S.T.A.R.	
		☐ Other:	
Department			
☒ Administrative Services	☒ Behavior Support	☒ Facilities	☒ QA/Compliance
☒ Finance	☒ Development	☒ Human Resources	☒ Research & Development
☒ IT	☒ Marketing & Communications	☒ Public Affairs	

POLICY

It is the responsibility and requirement of The Summit Center ("Summit"):

(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 Summit'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 Summit 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 Summit's data and data systems.

(6) to publish on its website a Bill of Rights for Data Privacy and Security that complies with the provisions of Education Law 2-d.

(7) Maintain a *Data Privacy and Security Plan* that Summit will include in contracts with Educational Agencies where Summit is the Third Party.

I. Standard

Summit will utilize the National Institute of Standards and Technology's Cybersecurity Framework v1.1 (NIST CSF or Framework) as the standard for its Data Privacy and Security Program.

II. Scope and Notice

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

This policy shall be published on Summit's website and notice of its existence shall be provided to all Summit employees, interns, volunteers, consultants and third parties who received or have access to Summit's SED data and/or data systems ("Users").

III. Compliance

Program Supervisors are responsible for the compliance of their programs 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's will be directed to adopt corrective practices, as applicable.

IV. Oversight

Summit's Data Protection Officer ("DPO") shall annually report to Summit's Operating Board 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.

V. 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 Summit policies to ensure it is protected from unauthorized use and/or disclosure.

(3) Summit has established a Privacy and Security Team to manage its use of data protected by law. The Data Protection Officer and the Privacy and Security Team will, together with Summit programs, 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 Summit procedures.

(6) It is Summit'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, Summit shall ensure that its contracts require that the confidentiality of student data or 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.

(8) PII sent to any party outside of Summit's secure network must be sent encrypted.

(9) Information that may contain student sensitive information must be placed in a clearly marked shredding bin for secure disposal.

VI. Incident Response and Notification

Summit responds to data privacy and security incidents in accordance with its Information Security Policy Manual. The incident response process will determine if there is a breach. All breaches must be reported to the office of the NYSED Chief 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 Summit sensitive or confidential data related to student, teacher or principal PII or a data system that stores that data, by or to a person not authorized to acquire, access, use, or receive the data.

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

VII. Other Summit Policies

Users must comply with Summit's ***Information Security Policy Manual #04001*** which outlines, but is not limited to, the responsibilities of all users of Summit's information systems to:

(1) maintain the security of the systems and to safeguard the confidentiality of PII,
(2) to comply with acceptable use of IT resources,
(3) to comply with access level requirements/limitations related to job responsibilities and minimum necessary access in order to accomplish tasks for Summit,
(4) to comply with account password policies,
(5) to comply with remote work and mobile device requirements.

VIII. Training

Summit Users must complete upon hire/onboarding and on an annual basis, information privacy and security training on the federal and state laws that govern the confidentiality of PII.

DEFINITIONS

Breach means the unauthorized acquisition, access, use, or disclosure of student data and/or teacher or principal data by or to a person not authorized to acquire, access, use, or receive the student data and/or teacher or principal data.

Personally Identifiable Information **("PII")** as applied to student data, means personally identifiable information as defined in §99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C. 1232g, and as applied to teacher and principal data, means personally identifiable information as such term is defined in Education Law §3012-c (10). PII includes, but is not limited to:

- *The student's name.*
- *The name of the student's parent or other family members.*
- *The address of the student or student's family.*
- *A personal identifier, such as the student's social security number, student number, or biometric record.*
- *Other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name.*
- *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.*

Teacher or Principal Data means personally identifiable information from the records of an education agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§3012-c and 3012-d.

Users means Summit employees, interns, volunteers, consultants and third parties who received or have access to Summit's data and/or data systems.

REFERENCES: LAWS, REGULATIONS, SUB-REGULATORY GUIDANCE

- NYS Education Law §2-d
- 8 NYCRR 21

RELATED POLICIES / PROCEDURES / FORMS / ATTACHMENTS

- #04001 Information Security Policy Manual
- #00140 General Confidentiality and Texting Policy
- Parents Bill of Rights Notice (10,100B)
- Data Security and Privacy Plan (10,100C)

DISTRIBUTION

Employees, interns, volunteers, consultants and other third parties who received or have access to Summit's PII; QA/CC Administrator (this policy to be posted on external website if updated).

HISTORY

Revised/ Reviewed Date	Summary of Change	Approver Title	Approver Date/Initials
4/22/2021	•Added requirement to have Summit's Parents Bill of Rights. •Data Security and Privacy Plan added to contracts with Educational Agencies when Summit is considered a third party. •Added website posting to Distribution list.	CEO	SRA 4/22/21
		CIO/IT Manager	WS/DP 4/22/21
		Corp. Compliance & Privacy Officer	CAD 4/22/21
1/5/2021	New policy	CEO	SRA 01/04/2021
		CIO/IT Manager	DP 01/05/2021
		Corp. Compliance & Privacy Officer	CAD 01/05/2021