SC ECIDS DATA GOVERNANCE MANUAL

Number: Title	Data Privacy and Confidentiality Policy		
Approved by	Early Childhood Advisory Council	Approved Date	10/17/2024

POLICY STATEMENT

The South Carolina (SC) Early Childhood Advisory Council (ECAC), as the governing body of the South Carolina Early Childhood Integrated Data System (ECIDS), is fully committed to ensuring that any information on young children, their families, or the programs and services in which they participate is kept private and confidential when used by external entities. Information from the SC ECIDS initiatives should be used to make decisions at a group or population level so that multiple young children, families, or programs can benefit. If the integrity or effectiveness of the SC ECIDS security measures or data is compromised, ECAC staff and the DGWG will take immediate corrective actions to mitigate the problems based upon applicable response processes. The ECAC will also be notified of any corrective actions within 3 business days.

PURPOSE

The purpose of this policy is to document how the SC ECIDS framework will ensure data assets are continually kept private, confidential, and secure when shared, used, or reported, as required by federal and state privacy and confidentiality laws. This policy allows the public to have confidence in the processes set up to protect data on children, families, and programs. This policy does not detail how external/authorized users access the data, as outlined in the "Data Access and Acquisition Policy."

SCOPE

This policy applies to all data collected, processed, and stored for each of the SC ECIDS initiative, including but not limited to personally identifiable information (PII), sensitive educational records, research data, and administrative data.

DEFINITIONS

- **Personally Identifiable Information (PII)** is any data that could potentially identify an individual, including names, addresses, social security numbers, or other identifying information.
- **Sensitive educational records** include data or information that are collected and stored for educational purposes that individual(s) may not want to be shared with others or could contain information that may cause harm to the individual.
- **Research data** are pieces of information that are collected for the purposes of conducting research or answering a research question, which could include data that have been adjusted based on administrative data or primary data collected for the purposes of conducting research.
- **Administrative data** is information about individuals or program operations that are collected and maintained as a part of the functioning of a service or program.
- **Participating programs** are programs that regularly contribute data to SC ECIDS.
- **External/authorized users** are individuals or entities granted access to ECIDS data for legitimate purposes, including researchers, policymakers, program administrators, and other stakeholders involved in early care and education.
- **Data sharing agreements (DSA)** are formal contracts or agreement between data owners and the SC ECIDS. This agreement outlines the terms and conditions under which data may be accessed, used, and disclosed, as well as the rights and responsibilities of each party with respect to the data.
- **Data breaches** are any incident in which unauthorized parties access, or obtain the ability to access, data that infringes upon the confidentiality and/or privacy of the data sources.

SC ECIDS DATA GOVERNANCE MANUAL

ROLES AND RESPONSIBILITIES

- **Participating programs** are responsible for submitting data stewards to serve on the Data Governance Work Group (DGWG), who are responsible for managing and maintaining data privacy and confidentiality standards specific to their program.
- **External/authorized users** are responsible for abiding by SC ECIDS data privacy and confidentiality policies.
- The **DGWG** is responsible for outlining, monitoring, and maintaining data privacy and confidentiality guidelines for SC ECIDS data.
- The **Data Governance (DG) Coordinator** is responsible for facilitating and managing decisions and recommendations of each DGWG, enabling decision-making, and aiding in issue resolution.

PROCESS

- The DGWG data stewards will compile information from their participating programs around data privacy and confidentiality guidelines which will be shared with the DG Coordinator.
- The DGWG data stewards will determine if there are other federal, state, or local regulations about data privacy and confidentiality (e.g., FERPA or HIPAA) related to their participating program's data which will be shared with the DG Coordinator.
- The DGWG, facilitated by the DG Coordinator, will align expectations across participating programs within the parameters of the privacy and confidentiality policies of the appropriate technical lead(s) as outlined in the DSAs (for example, see the SC Department of Education (SCDE) Security Policies for the Early Learning Extension (ELE) initiative).
- The DG Coordinator will develop processes for communicating these guidelines with the ECAC, DGWG, participating programs, and any external/authorized users of SC ECIDS through the ECIDS Data Hub website.
- The DGWG will abide by the data suppression, data storage, and data breach processes to support privacy, security, and confidentiality under the SC ECIDS framework.

DATA SUPPRESSION

- Any report or other publication produced within the SC ECIDS framework must use appropriate disclosure avoidance techniques to protect individually identifiable information. No cell, table or text discussion can include information that pertains to 10 or fewer children or families.
    - Complementary suppression of non-sensitive cells may also be required so that suppressed values of 10 or fewer cannot be calculated by subtracting reported values from row and/or column totals.
- Based on the specifics of the analysis, additional disclosure avoidance techniques such as aggregation across categories may be necessary. Data users should consult with the DG Coordinator in these cases.
- Reports and publications using data assets from SC ECIDS initiatives produced by external/authorized users are subject to additional pre-submission review (see "Data Analysis and Reporting Policy") to ensure adequate data suppression.

DATA STORAGE

- Data requesters and users will adhere to best practices for storage and encryption of data to minimize any risk of data being transmitted to an unauthorized person or location.

DATA BREACH RESPONSE PROCEDURE

- If a data breach is suspected or occurs within an SC ECIDS application:
  - The technical lead(s) will notify the DG Coordinator.
  - The DG Coordinator will notify the ECAC and DGWG members from the impacted participating programs within three business days of learning of the incident.
  - Because data is being stored with the technical leads of each SC ECIDS initiative, the response process will follow the processes and procedures outlined in the privacy and confidentiality policies of the technical lead(s) and will be supported by ECAC staff.
  - The technical leads, with support from the DG Coordinator and ECAC staff, will be responsible for making any public notices of data breaches needed beyond those covered by their own privacy and confidentiality policies.
  - The DG Coordinator, in collaboration with the technical lead(s) and ECAC staff, will notify impacted participating programs and the ECAC of corrective actions within three business days.
- If an external/authorized user or participating program is involved in a data breach related to an SC ECIDS initiative:
  - The party must report it to the DC Coordinator within three business days from the date they were made aware of the breach.
  - The DG Coordinator will notify the appropriate technical lead(s), the DGWG, and the ECAC within three business days.
  - The DGWG, in conjunction with the technical lead(s) and ECAC staff, may require the party involved to investigate and respond to questions regarding the data breach.
  - The DGWG, in conjunction with the technical lead(s) and ECAC staff, may require the party involved to promptly resolve any issues uncovered by the investigation.
  - Members of the DGWG or the DG Coordinator may also request the formation of a Data Breach Project Team (See “Establishment of Project Teams Policy”) to devise long-term solutions to issues uncovered in the investigation, if applicable.
  - The DGWG, in conjunction with the technical lead(s) and ECAC staff may require the party involved to submit a corrective plan with steps to prevent any future unauthorized disclosures or data breaches.
  - If the party involved fails to comply with response processes, the DGWG and/or technical lead(s) may restrict their access to SC ECIDS data assets in the future.
  - The DG Coordinator, in collaboration with the technical lead(s) and ECAC staff, will notify impacted participating programs and the ECAC of corrective actions.

RELATED POLICIES

- Data Access and Acquisition Policy
- Data Scope and Management Policy
- Data Analysis and Reporting Policy
- SCDE Security Policies

REVISION HISTORY

Responsible Party	Reason for Change	Date	Version
Molly Tuck	Revision 1 of policy shared with DGWG	August 28, 2024	1.1
Molly Tuck	Initial Version of Policy	August 7, 2024	1.0

SC ECIDS DATA GOVERNANCE MANUAL