**Glossary of Defined Terms**

# Purpose

This document includes an alphabetical list of **terms** with the **definitions** for those **terms** utilized for SLEDS.

# Scope

This Glossary applies to SLEDS Policies and Procedures. For additional defined terms used in SLEDS Policies, see the [ETS Glossary](https://docs.google.com/document/d/1l72ZchJxazqZKv2um89YTqoQ6rQd3qdjFzDOx0Kcn7o/view#).

## Defined Terms

| **Term** | **Definition** | **Policy/Procedure** |
| --- | --- | --- |
| Advisory Member | An organization that is not a Participating Entity and serves as a non-voting member of a committee, team, or workgroup within the SLEDS Governance Structure for the purpose of advising the committee, team, or workgroup of matters within the organization’s subject matter expertise. | Awareness and Training Policy |
| Advisory Member Organization | The organization to which the Advisory Member belongs and represents in the SLEDS Governance Structure. | Awareness and Training Policy |
| Anonymized data | Student data elements from which all direct and indirect identifiers have been removed. Anonymized data will often still contain PII. Anonymized data is not synonymous with De-identified data. | MOU  Data Destruction Policy  Personnel Security Policy |
| Authorized User | Employees of the Parties who have been approved by the Data Governance Committee to have access to PII in the WCCCE for the purpose of carrying out the study established by this MOU. | MOU |
| Confidential Information | Information that may include, but is not limited to, Personally Identifiable Information (PII) as defined by FERPA, information that contains PII as defined in WPRA, and employee information. Disclosure of this information is subject to SLEDS MOUs and Non-Disclosure Agreements and cannot be disclosed outside of the SLEDS Governance Structure without prior written approval in accordance with Federal and State privacy laws. This information has been anonymized and combined with other PEs data. | Awareness and Training Policy  Data Classification Policy  Identification and Authentication Policy  Participating Entity Confidentiality Statements  Personnel Security Policy |
| Data | Expressed information representing facts in a variety of qualitative and quantitative forms, including aggregate, individual level, and Personally Identifiable Information (PII). |  |
| Data Custodian | The entity (WCCC) which manages and maintains the data for the SLEDS data and information once it has been transmitted to WCCC. | Incident Response Procedure  Access Control Procedures |
| Data Dictionary | A compendium of data definitions for multiple data elements that exist in a data store. |  |
| Data Files | Data files are physical and electronic representations of information, and any copies made. Examples of data files include but are not limited to:   * Hard drives * Networking equipment * Paper printouts * Flash drives * Institutional servers * Any other media or type of materials that store, capture, or process data | Data Destruction Policy |
| Data Sharing Agreement | Legal documents between two or more parties that codify the terms and conditions for the sharing and use of data. SLEDS requires agreements when disclosing Personally Identifiable Information (PII) from education records with third parties. |  |
| Data Stewards | Entity providing data to the SLEDS program. | Incident Response Procedure  Access Control Procedures |
| De-Identified Data | The Process of removing or obscuring any PII from a dataset in a way that minimizes the risk of unintended disclosure of the identity of individuals and information about them. While it may not be possible to remove the disclosure risk completely, de-identification is considered successful when there is no reasonable basis to believe that the remaining information in the records can be used to identify any individual. De-identified data may be shared without the consent required by FERPA (34 CFR §99.30) with any party for any purpose, including parents, general public, and researchers (34 CFR §99.31(b)(1)). [See PTAC Overview of Data De-identification](https://studentprivacy.ed.gov/sites/default/files/resource_document/file/data_deidentification_terms_0.pdf). | MOU  Access Control Procedures |
| DMZ | Demilitarized Zone - Perimeter network segment that is logically between internal and external networks. Its purpose is to enforce the internal network’s Information Assurance policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the internal networks from outside attacks.  Source (https://csrc.nist.gov/glossary/term/demilitarized\_zone) |  |
| ETS | The Wyoming Department of Enterprise Technology Services. ETS performs IT services for various Wyoming state agencies. | MOU |
| Event | An event is an observed or observable occurrence in a system, a network, or daily operations. Events are not necessarily adverse. When first observed, an event could appear to be an incident but after analysis, could turn out to be an explainable and defendable anomaly in the environment. An event (‘something happened’) will typically occur prior to the declaration of a ‘security incident.’ Until events are declared adverse, they can be called ‘events’ or ‘suspected incidents.’ | Incident Response Policy |
| Family Educational Rights and Privacy Act (FERPA) | A federal law (20 U.S.C. § 1232g; 34 CFR Part 99) that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education. FERPA gives parents certain rights with respect to their children's education records, including the right to have access to their children’s education records, the right to seek to have the records amended, and the right to consent to the disclosure of PII from education records, except as provided by law. These rights transfer to the student when he or she reaches the age of 18 or attends a school beyond the high school level. Students to whom the rights have transferred are eligible students. |  |
| High Availability Data System MOU (HADS) | The common name used to refer to the MOU, and its amendments, written to allow the Statewide Longitudinal Education Data System (SLEDS) to collect and link student-level and workforce data in a data system to audit and evaluate educational programs under the purview of the Parties to this MOU in accordance with Wyo. Stat. Ann. § 21-18-202(a)(vi)(C). This includes developing analytical reports and providing statistical data about these efforts so that the legislature and participating agencies can make informed decisions about the educational programs and services within their purview. |  |
| Incident | An incident is an event that negatively affects the confidentiality, integrity, and/or availability (CIA) at an organization in a way that impacts the business. | Audit and Accountability Policy  Incident Response Procedure  Incident Response Policy |
| Information Owner | The agency, entity, or organization appointed by the SLEDS Governance Structure to have access to the WCCCE or submit data to the WCCCE for the purpose of submitting, managing, or updating SLEDS data. The Wyoming Community College (WCCC) shall serve as the Information Owner of data within the WCCCE and each Participating Entity will serve as the Information Owner of the data to the point of submission to WCCCE. |  |
| Information Security Incident | Need definition. Should align with [Wyoming Security Incident Declaration Guideline 09400-G191C](https://drive.google.com/file/d/0B_YE8dWRQWQAWWR4c2NfbDRzcGc/view?resourcekey=0-dVvtiglpo4flmZzsqOyjrw) | Incident Response Policy |
| Information System Owner | The entity in charge of one or more systems, each of which may contain and operate PII, anonymized data, and other data defined in X. An Information System Owner is in a position that predisposes the entity to participate in drafting security policies, supporting procedures, standards and baselines, and to disseminate them among Participating Entities. ETS shall serve as the Information System Owner for the SLEDS WCCCE | Incident Response Procedure |
| Internal Information | Information whose loss, corruption, or unauthorized disclosure is of importance only inside the State and, therefore, would not result in a tangible business, financial or legal loss. This information has been fully anonymized, de-identified, aggregated, but not authorized for public release. | Data Classification Policy |
| Levels of Access | The following levels of access have been developed based on the data classification definitions. For each access level, approved staff must fulfill training requirements established by WCCC and the SLEDS DGC. A complete list of individuals with access to SLEDS by level will be maintained by the WCCC Security Team. The access levels listed below are in the order of the most restrictive to the least restrictive:   * ***PII Access WCCC (SLEDS Staging Server)*** – allows specific WCCC IT staff to read and write to records and fields in the WCCCE. This access level is only permitted to a minimal number of authorized staff members who operate or manage the WCCCE or are responsible for maintaining the accuracy and security of the data in the performance of their duties. Approval of access is granted by WCCC Security Team (CTO, Business Applications Analyst, and Business Analyst) upon training, background checks, and signing of the appropriate data sharing agreements. * ***PE PII Access (SLEDS* Staging Server -Single Agency Database with row level security)** – allows a Database Analyst / Developer from each PE to access specific records and fields within WCCCE in order to validate appropriate data linking and manage error reporting upon submission of data to WCCCE and maintain the accuracy and security of the data in the performance of their duties. Row-level security is employed so that each PE is only able to see their own data and their role is strictly Quality Control (not research). Access is determined by the Data Governance Committee (DGC) and in alignment with SLEDS Data Sharing MOU(s) and the Personnel Security Policy. The PE’s designated security representative approves access for the designated individual. Approval by the WCCC Chief Technology Officer is also required. * ***SLEDS Combined Anonymized Relational Database Access (Staging Server)*** – All data except for PII data elements will be copied via SQL insert statements from the SLEDS PII Database to the SLEDS Anonymized Database. The Anonymized ID will exist in all tables in lieu of all other IDs (i.e. local agency assigned IDs, SSN, etc.) person name, birthdate and gender. A new Anonymized ID will be generated daily and updated in the SLEDS Anonymized Database. Database Analyst / Developer access is determined by the Data Governance Committee and in alignment with SLEDS Data Sharing MOUs and the data confidentiality policy, and their role is strictly Quality Control (not research). Row-level security is employed so that each Participating Entity is only able to see their own data. * ***SLEDS PE Anonymized Relational Database Access (Production Server)*** – allows a minimal number of authorized research and data stewards of PE’s to access data included in the reports with SLEDS anonymized data. Suppression rules must be utilized by the researcher in production of summary level reports. Access is determined by the DGC and in alignment with SLEDS Data Sharing MOU(s) and the Personnel Security Policy. Researcher access is determined by the Data Governance Committee. * ***SLEDS De-Identified Data Access (Production Server)*** – allows access for designated staff to SLEDS de-identified data and secured reports consistent with best practices, state and federal law. Approval of access is granted by the PEs upon recommendation of the SLEDS DGC. Suppression rules must be utilized by the researcher in production of public reports. * ***Public Reporting Report/Dashboard Access*** – allows access to the DGC and E-Board approved report to the general public for viewing standard summary SLEDS data. | Access Control Procedures |
| Participating Entity | Agency, entity, or organization that has signed the SLEDS Memorandum of Understanding to share or contribute data into the WCCCE. |  |
| Participating Member | An employee, contractor, or other Participating Entity personnel to be nominated or appointed by a Participating Entity to fulfill key roles within the SLEDS Governance Structure or complete identified tasks on behalf of the Participating Entity for the SLEDS Program. |  |
| Participating Entity Information Owner | The agency, entity, or organization appointed by the SLEDS Governance Structure for the purpose of managing and updating SLEDS data to have access to the WCCCE or submit data to the WCCCE. The Wyoming Community College (WCCC) shall serve as the Information Owner for managing SLEDS data within the WCCCE and other Participating Entities will serve as the Information Owner of the data to the point of submission to WCCCE. | Incident Response Procedure |
| Personally Identifiable Information (PII) | For purposes of SLEDS Policies, PII means any and all student information contained in the student data elements that falls within the definition of Personally Identifiable Information in 34 C.F.R. § 99.3 and includes, but is not limited to:   * A student name * The name of the student's parents or other family members; * The address of the student or student's family * A personal identifier such as the student’s date of birth, place of birth, and mother’s maiden name * Other indirect identifiers 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 * 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 | MOU  Incident Response Procedure |
| Project Manager | An individual responsible for managing a project with firm start and end dates. |  |
| Public Information | Information that poses no risk to the State or individuals represented by the data if the information is made generally available. This information has been fully anonymized, de-identified, aggregated and authorized for public release. | Data Classification Policy |
| Restricted Information | Information that may include, but is not limited to, Personally Identifiable Information (PII) as defined by FERPA, information that contains PII as defined in WPRA, and employee information. Disclosure of this information is subject to SLEDS MOUs and Non-Disclosure Agreements and cannot be disclosed outside of the SLEDS Governance Structure without prior written approval in accordance with Federal and State privacy laws. This information has **not** been anonymized and only the sourcing PEs can see this data within the SLEDS database | Data Classification Policy |
| School Official | An entity or individual receiving PII that is performing institutional services or functions for which an institution would otherwise use employees, that is under the direct control of the institution with respect to the use and maintenance of education records and PII disclosed by an institution under this agreement, that is only allowed to use PII disclosed by an institution under this agreement for the purposes for which the disclosure is made, and is not allowed to disclose PII provided under this agreement except in accordance with 34 CFR 99.33. |  |
| Security Event | An event is an observed change to the normal behavior that impacts or has the potential to impact SLEDS, including the WCCCE, processes, access, workflow or person. | Incident Response Procedure  Incident Response Policy |
| Security Managers | The joint role of WCCC and ETS for data and application security. | Incident Response Procedure  Access Control Procedures |
| SLEDS | The statewide longitudinal education data system established pursuant to Wyoming Statute § 21-18-202(a)(vi)(C). | MOU |
| SLEDS Governance Structure | Collectively or individually, the various committees, subcommittees, workgroups, teams, or any other group of individuals who are convened on behalf of the SLEDS Program to represent or work on behalf of the Participating Agencies. This includes, but is not limited to, the frameworks, structures, policies, and practices that define management principles, oversight functions, and decision making concerning the SLEDS Program, WCCCE, or SLEDS Information. |  |
| SLEDS Data Product | A report, study, visualization, spreadsheet, dataset or any other information or deliverable produced from the WCCCE using SLEDS Information for the purpose of ultimately being shared outside the SLEDS Governance Structure. A Final SLEDS Data Product connotes such deliverable that has been so shared. |  |
| SLEDS Data Stewards | Participating Entity staff tasked with fulfilling certain duties or responsibilities identified in the SLEDS Policies including tasks within the Data Research Request Process, or other tasks as requested through the SLEDS Data Governance Structure. SLEDS Data Stewards shall be members of the Privacy Subcommittee, Research Subcommittee, and/or Data Stewards and Standards Subcommittee, unless or until the alternate individuals are identified and appointed through the SLEDS Governance Structure. |  |
| WCCCE | Information technology resources and infrastructure components containing, extracting, transforming, or loading SLEDS Information. Such resources include the hardware and data storage maintained and/or hosted in the Greenhouse Data Center, as well as the software, firmware, applications, security tools, data or business intelligence tools, and networks connected to such infrastructure components. |  |
| SLEDS Information | Structured and unstructured data in whatever form or medium that is contained within--or sourced from--the WCCCE. |  |
| SLEDS Security Team | The Wyoming Department of Enterprise Technology Services (ETS) and/or Participating Entity staff responsible for fulfilling certain duties or responsibilities identified in SLEDS Policies, or as otherwise requested through the SLEDS Data Governance Structure. Members of the SLEDS Security Subcommittee shall serve as members of the SLEDS Security Team unless or until the alternate individuals are identified and appointed through the SLEDS Governance Structure. |  |
| SLEDS Policies | The collective set of policies, standards, processes, and procedures that have been formally approved, adopted, or ratified by the SLEDS Data Governance Committee or as otherwise approved through the SLEDS Data Governance Structure. |  |
| SLEDS Program | See, e.g. Participating Member Confidentiality reference. |  |
| State Policy | Used to reference State of Wyoming policies for Data, Privacy, Cyber Security and other Information Technology and Data Management related policies. | Used in SLEDS Policies, Procedures and other Documentation |
| Third Party | Used in the context of data, an individual, entity or organization external to the Participating Entity having ownership of the data in question. This may include, for example, a Participating Member from a Participating Entity. |  |
| WCCCE | The WCCC environment inclusive of technical architecture and processes. This includes the environments and processes for transforming PII data to Anonymized datasets and ultimately De-Identified datasets. | MOU  Access Control Procedures |
| Wyoming Public Records Act (WPRA) | Wyoming Statute 16-4-201 through 205, as amended. | Data Classification Policy |