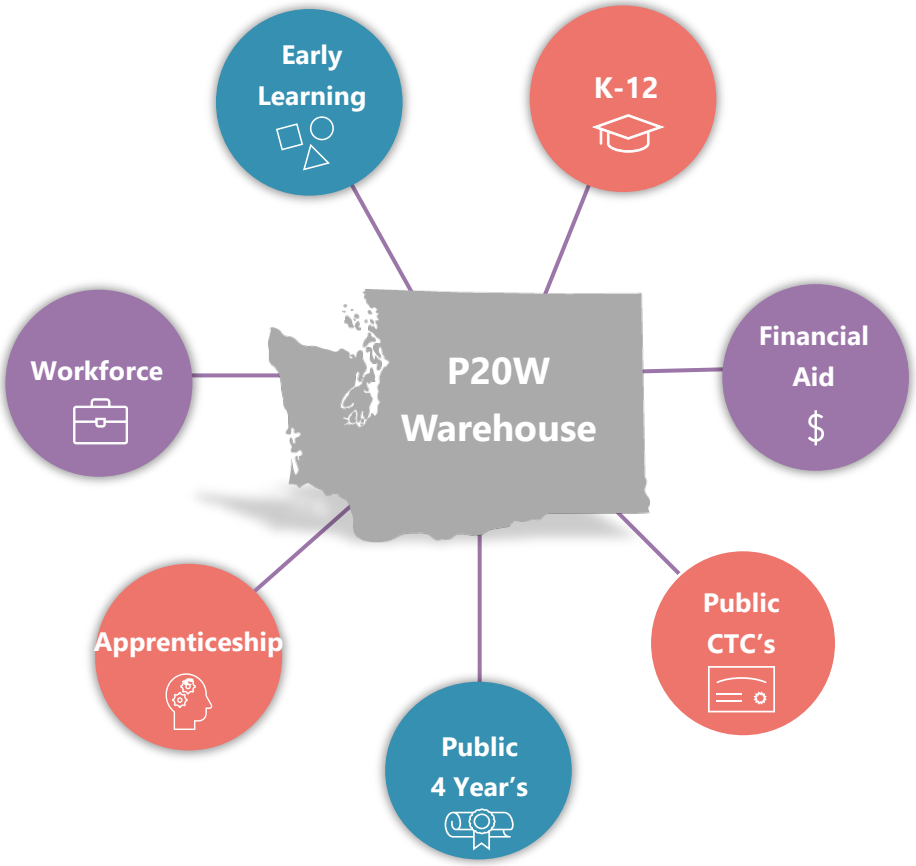
Data Governance Manual

November 2024



Education Research and Data Center
Forecasting and Research
Office of Financial Management

About the ERDC

ERDC works with data contributing agencies and the education research community to fulfill data requests, create dashboards, and conduct research to better understand the education systems in the state. The legislature assigned specific requirements for ERDC in its originating legislation, RCW 43.41.400. ERDC engages in a number of activities, including but not limited to: creating data products, analyzing data and reporting for state agencies, conducting cross-sector research, and supporting data collections.

Address

Education Research and Data Center
1500 Jefferson St. SE
Olympia, WA 98501

Phone

360-902-0599

Email

erdc@ofm.wa.gov

Revision History

Date	Version #	Author	Comments
8/1/2022	1.0	Bonnie Nelson	Original Version
3/12/2024	1.1	Bonnie Nelson	Changed Data Contributor Opportunities to Partnership Opportunities; Updated Internal Review Process
11/8/2024	1.2	Katie Weaver Randall	Removed Internal Fulfillment Section; Updated ERDC privacy principles; Updated ERDC required trainings.

Table of Contents

Purpose & Background

This is the State of Washington Office of Financial Management's (OFM) Education Research and Data Center's (ERDC) P20W Statewide Longitudinal Data System Data Governance Program. This document serves to describe and document the ERDC governance structure. This document will be reviewed and updated on an annual basis as business, technical, and people roles evolve.

At ERDC, we build and maintain a P20W longitudinal data system by partnering with other state agencies throughout the state who contribute data to ERDC. The purpose of this longitudinal data system is to enable researchers at ERDC and elsewhere to conduct valuable research that informs policy- and decision-making both at the state level and within partnering institutions. Individuals and organizations throughout the state, including state policymakers, school superintendents, school principals, university administration, and academic researchers, benefit from the research conducted by researchers at ERDC.

During the 2007 session, the Washington Legislature passed a bill that created the Education Research & Data Center (ERDC) in the Office of Financial Management. The aim of ERDC was to make education data available to policymakers and state organizations that make decisions related to Washington students, while also protecting the privacy of students. ERDC was partnered with the Legislative Evaluation and Accountability Program (LEAP) Committee to conduct analysis of early learning, K-12, and higher education programs across the P-20 system and into the workforce.

ERDC compiles data about students as they move through school to the workforce. As the home for the statewide longitudinal data system (SLDS), ERDC works with partner agencies to develop analyses of education systems that can improve student outcomes. These sectors include early learning, K-12, post-secondary, and workforce sectors, which are referred to collectively as P20W (preschool to grade 20 to workforce). In this way, ERDC acts as a kind of "central hub," where partnering agencies, institutions, and organizations can pool their data and seek answers to questions that none of them have the resources to answer by themselves.

Vision

To promote a seamless, coordinated preschool-to-career (P-20W) experience for all learners by providing objective analysis and information.

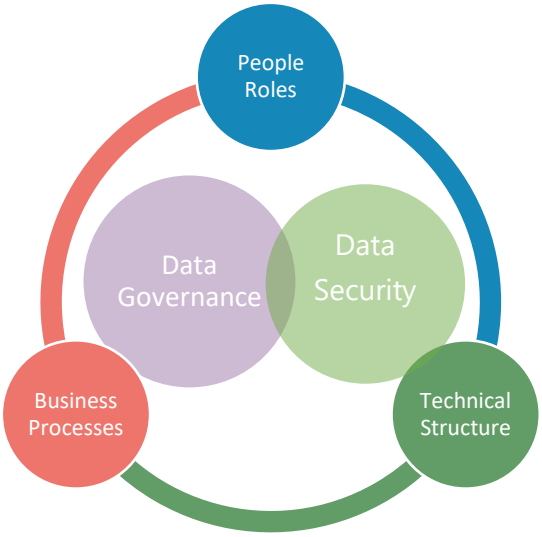
Mission

To develop longitudinal information spanning the P-20W system in order to facilitate analyses, provide meaningful reports, collaborate on education research, and share data.

P20W Data Governance & Data Security Overview

Data Governance and Data Security are two interconnected, yet distinct programs that ensure the privacy and safekeeping of data that enters and leaves the ERDC P20W. Each program involves People Processes, Business Processes, and Technical Structures.

Figure 1. Conceptual relationship of data governance and data security



Data Governance for the P20W statewide longitudinal data system (SLDS) is documented through:

1. Business & Technical Processes: Our business processes related to data sharing are rooted in the compliance of state and federal laws that ensure student privacy, as well as proper access, use, and storage of data. Technical solutions are embedded within our business processes for fulfilling data requests to maintain limited access and the safe exchange of data with contributors and requestors.

2. People Roles: Our governance ensures that staff meet professional standards for privacy and data use, that we involve our data contributors, and we maintain relationships with informed data requestors.

Data Security for the P20W statewide longitudinal data system (SLDS) is documented through:

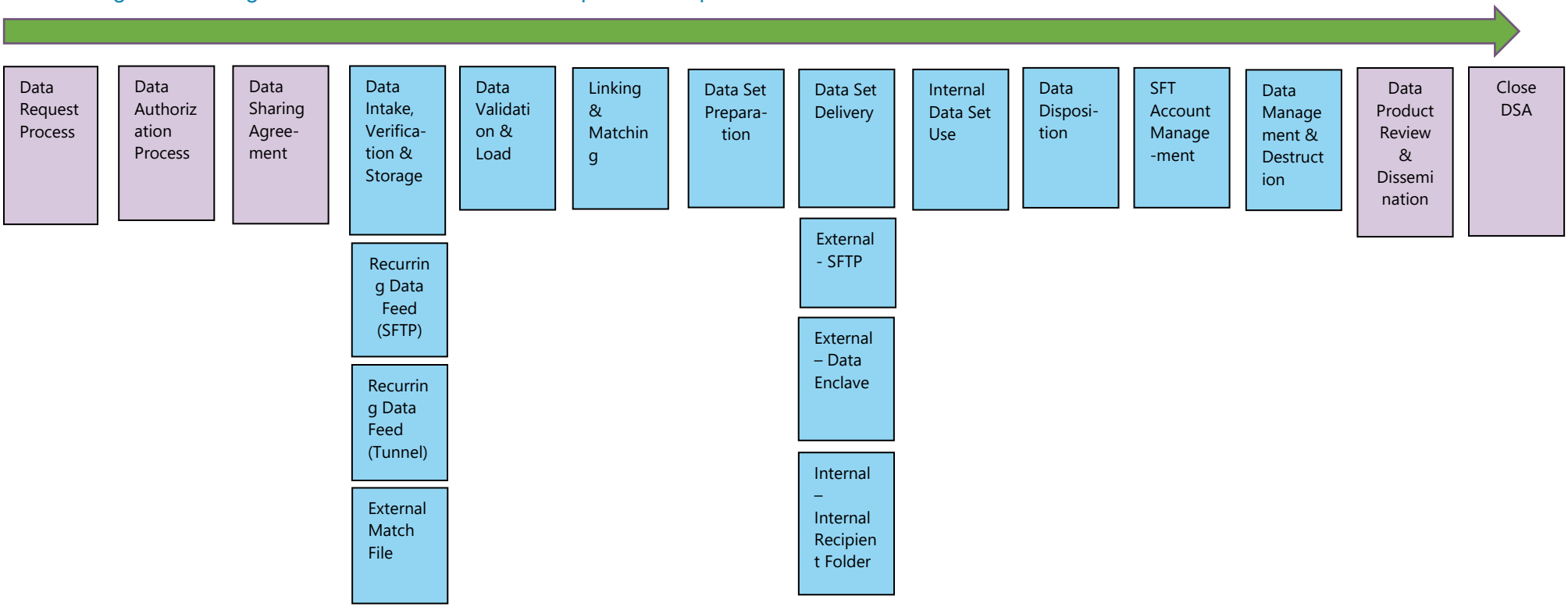
1. Business & Technical Processes: Our business processes are designed to ensure the security of P20W data as it moves from ERDC partners, to the ERDC and on to data requestors, as well as data from requestors to the ERDC. This includes technical structures to protect the data and communications networking components, connections and contents; protecting the physical items, objects from unauthorized access or misuse.

2. People Roles: ERDC staff and contractors who access and/or work with the either the P20W data or system or both in a research or technical capacity.

ERDC's P20W Data Governance and Data Movement Process Map

ERDC's business processes are performed with the goal of providing P20W data products to requestors. The business processes are categorized as either Data Governance (purple boxes) or a Data Movement (blue boxes) activity. This document describes the **data governance processes**. Data movement processes are outlined in the Data Security Manual.

Figure 2. Data governance and data movement process map



Key Terms when working with ERDC P20W data

The following terms were retrieved from the student Privacy Policy Office's Privacy Technical Assistance Center in the US Department of Education at https://studentprivacy.ed.gov/glossary.

Table 1: Key PTAC Definitions

Term	Definition from PTAC
Education Records	Education records are those records that are directly related to a student and are maintained by an educational agency or institution or by a party acting for the agency or institution.
Personally identifiable information (PII)	Any information, such as a name or identification number, that can be used to distinguish a person's identity. This may be through **direct identifiers**, such as name or ID number, or through **indirect identifiers**, such as a student's date of birth, or other information which can be used to distinguish or trace an individual's identity through linkages with other information.
Direct Identifier	Direct identifiers include information that relates specifically to an individual such as the individual's residence, including for example, name, address, Social Security Number or other identifying number or code, telephone number, e-mail address, or biometric record.
Indirect Identifier	Indirect identifiers include information that can be combined with other information to identify specific individuals, including, for example, a combination of gender, birth date, geographic indicator and other descriptors. Other examples of indirect identifiers include place of birth, race, religion, weight, activities, employment information, medical information, education information, and financial information.
Disclosure	Disclosure means to permit access to or the release, transfer, or other communication of **personally identifiable information (PII)** by any means (34 CFR §99.3). Disclosure can be Authorized, such as when a parent or an eligible student gives written consent to share education records with an authorized party (e.g., a researcher). Disclosure can also be Unauthorized or inadvertent (accidental). An unauthorized disclosure can happen due to a data breach or a loss, and an accidental disclosure can occur when data released in public aggregate reports are unintentionally presented in a manner that allows individual students to be identified.
Disclosure Avoidance	Disclosure avoidance refers to the efforts made to de-identify the data in order to reduce the risk of disclosure of **personally identifiable information (PII).** A choice of the appropriate de-identification strategy (also referred to as **disclosure limitation method**) depends on the nature of the data release, the level of protection offered by a specific method, and the usefulness of the resulting data product. The two major types of data release are **aggregated data** (such as tables

	showing numbers of enrolled students by race, age, and sex) and **individual level data** (such as individual-level student assessment results by grade and school). Several acceptable de-identification methods exist for each type of data.
Disclosure Limitation Method	Disclosure limitation method (also known as disclosure avoidance method) is a general term referring to a statistical technique used to manipulate the data prior to release to minimize the risk of inadvertent or unauthorized disclosure of personally identifiable information (PII).
Identifiable data	*Identifiable data* includes any information that can be used to distinguish an individual. Even without **direct identifiers** (such as a name) a record-level dataset is not necessarily a de-identified dataset. Identifiable data is protected by FERPA and other privacy laws.
De-identifiable data	De-identified data describes records that have a re-identification code and have enough **personally identifiable information** removed or obscured so that the remaining information does not identify an individual and there is no reasonable basis to believe that the information can be used to identify an individual. The re-identification code may allow the recipient to match information received from the same source.
Redaction	Redaction is a general term describing the process of expunging sensitive data from the records prior to **disclosure** in a way that meets established disclosure requirements applicable to the specific data disclosure occurrence (e.g., removing or obscuring **PII** from published reports to meet federal, state, and local privacy laws as well as organizational data disclosure policies).
Suppression	Suppression is a disclosure limitation method which involves removing data (e.g., from a cell or a row in a table) to prevent the identification of individuals in small groups or those with unique characteristics.

Detailed P20W Business Processes: ERDC Roles & Compliance

How does ERDC fit into the state education landscape?

The ERDC is housed within the Forecasting & Research Division of the Office of Financial Management (OFM) (see Appendix for organization chart). OFM provides vital information, fiscal services and policy support that the Governor's Office, Legislature, and state agencies need to serve the people of Washington. The Office of Financial Management:

- Plays a central role in budget planning, policy development, and fiscal administration for the executive branch.
- Prepares the executive budget proposal and monitor budget implementation.
- Develops and maintains state administrative and accounting policies and prepare statewide financial reports.
- Conducts executive policy research and develop legislation to support the Governor's policy goals.
- Provides estimates of state and local population, monitor changes in the state economy and labor force, and conduct research on a variety of issues affecting the state budget and public policy.
- Manages statewide human resource policy functions including classification, compensation, workforce data, recruitment and other policy functions.
- Supports the state service commission (Serve Washington) whose goal is to improve lives, strengthen communities, and foster civic participation through service and volunteering.

ERDC functions as *both* an authorized representative *and* a State Education Authority. The legislature has established the ERDC, as a matter of state law, as an authorized representative of the state educational agencies. At the same time, ERDC is also a State Education Authority as determined by the activities that it performs for the state. The ERDC governance structure is rooted in these dual roles and this enables the ERDC to conduct the wide range of activities that are required of ERDC.

Roles & Ongoing Activities of ERDC

ERDC was created in 2007 and charged with the assignment track student progress and transitions through school, from preschool to college, in order to determine ways to improve student outcomes. This mission has been expanded over the years.

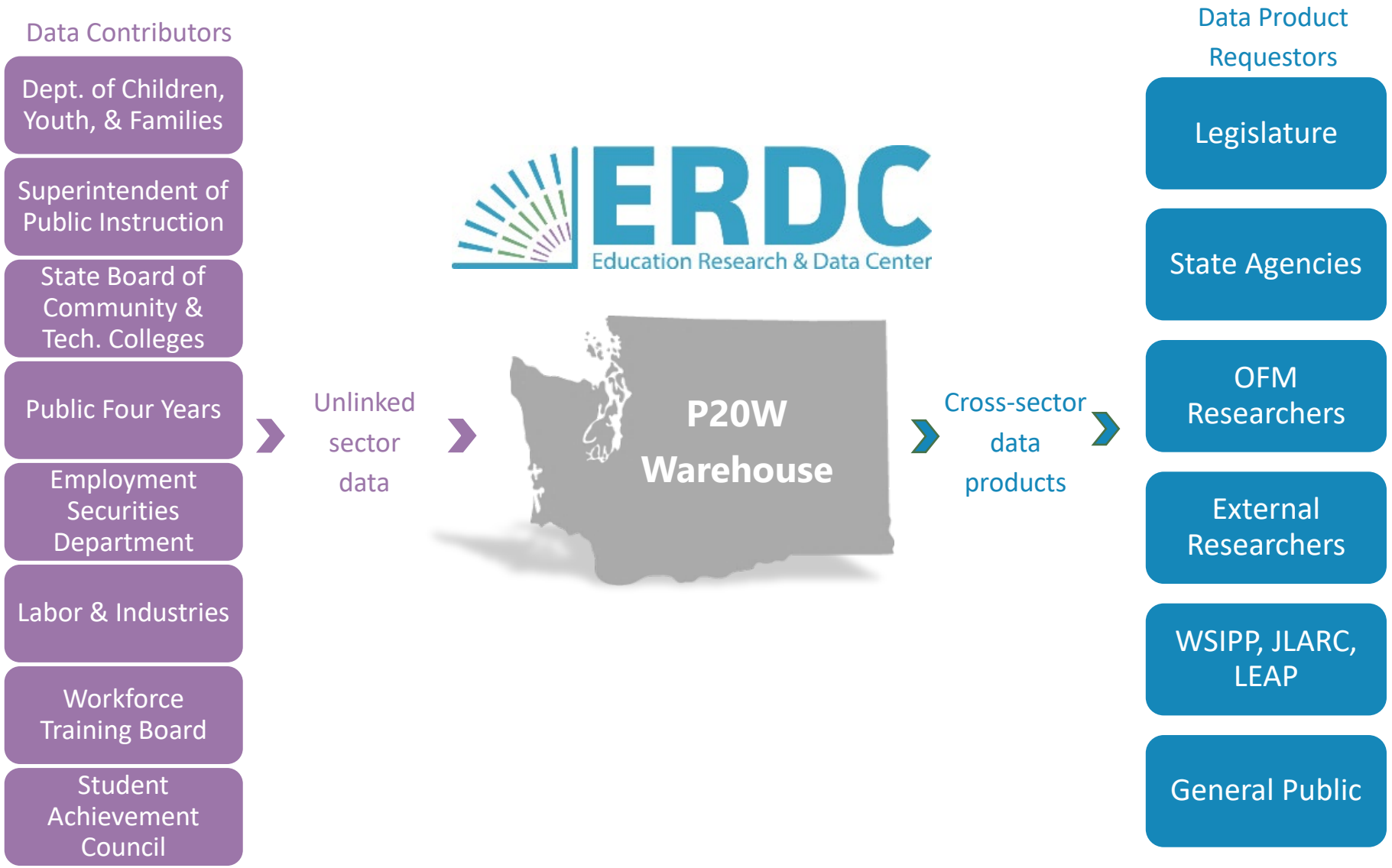
State Education Authority. The Family Policy Compliance Office has interpreted the term "state and local educational authorities" to mean, an agency or other party with educational expertise and experience that is responsible for and authorized under State or local law to regulate, plan, coordinate, advise, supervise or evaluate elementary, secondary, or postsecondary education programs, services, agencies, or institutions in the State. ERDC is responsible for the evaluation of state education programs in Washington across the P20 to workforce spectrum.

Authorized Representative. ERDC is established as an authorized representative of the state educational agencies for purposes of researching and analyzing data to support education budgeting and policymaking functions of the Legislature, the Governor, and state educational agencies.

Example Activities. The duties of ERDC are outlined by the legislature in RCW 43.41.400 (see below) and performed through our dual roles. In order to accomplish these duties, ERDC performs several regular activities, including but not limited to:

- Provide governance and oversight for the Statewide Longitudinal Data System and other data housed in ERDC systems, including submission, security and privacy considerations.
- Identify critical research and policy questions for education in Washington state.
- Assist with development of long-range enrollment plans for higher ed including estimates to meet demographics and workforce needs
- Provide data products that inform and advise the Governor's budget and policy office, OSPI, WSAC, DCYF, and other state agencies
- Support statewide education research through fulfillment of data requests from external researchers that are evaluations of education programs or studies conducted on behalf of a state or local education authority
- Update and maintain data resources, including data dictionaries and dashboards
- Provide legislative session support, including fiscal note preparation; data requests; presentations
- Manage the US Department of Education SLDS grant. This includes an annual report, site visits, conference presentations, and annual deliverables

Figure 3. Flow of data from data contributors, to ERDC, to the data product requestors.



Compliance with Federal Laws

This data governance plan establishes the rules for the access and use of data collected, stored, or maintained by the ERDC. This policy is consistent with the disclosure provisions delineated in the Federal Education Rights Privacy Act of 1974 (FERPA) and all other applicable state and federal data privacy laws.

Privacy laws govern how education and employment data can be shared. ERDC cannot release or share information about individuals that would constitute an unwarranted invasion of privacy. In compliance with these laws and regulations, ERDC only publishes aggregate information, and never information that can be used to identify individuals. Privacy laws and related guidance continue to evolve, and ERDC is committed to taking steps to update its processes to reflect these changes.

Federal law (specifically, the Federal Educational Rights and Privacy Act of 1974, also known as "FERPA") safeguards the confidentiality of individual student information. This law requires that educational institutions and state agencies maintain the confidentiality and privacy of personally identifiable information in student records. The U.S. Department of Education has created extensive regulations regarding implementation of FERPA under Title 34, Part 99 of the Code of Federal Regulations.

In some instances, data may also be protected by the Parts B and C of the federal Individuals with Disabilities Education Act, also known as "IDEA". Federal regulations regarding implementation of IDEA can be found in Title 34, Part 300 and Title 34, Part 303 of the Code of Federal Regulations. IDEA incorporates all the provisions of FERPA and adds eight additional requirements to safeguard privacy.

Workforce-related data are also protected and secured by federal law, such as Section 303 of the Social Security Act, for which the U.S. Department of Labor has promulgated Title 20, Part 603 of the Code of Federal Regulations. Furthermore, the federal Workforce Innovation and Opportunity Act of 2014 prohibits the disclosure information collected under the auspices of the workforce development system that would "constitute a clearly unwarranted invasion of personal privacy."

The following is a list of commonly referenced resources that guide the ERDC privacy practices and decisions related to FERPA compliance:

- FERPA Regulation, 2011 https://www2.ed.gov/policy/gen/guid/fpco/pdf/ferparegs.pdf
- Integrated Data Systems https://studentprivacy.ed.gov/resources/integrated-data-systems-and-student-privacy
- FERPA Guidance for Reasonable Methods and Written Agreements https://studentprivacy.ed.gov/resources/guidance-reasonable-methods-and-written-agreements
- SLDS Tech Brief #3: Statistical Methods for Protecting Personally Identifiable Information in Aggregate Reporting https://studentprivacy.ed.gov/resources/tech-brief-3-statistical-methods-protecting-personally-identifiable-information-aggregate
- IDEA-FERPA Confidentiality Provisions https://www2.ed.gov/policy/gen/guid/ptac/pdf/idea-ferpa.pdf
- Case Study #2: Head Start Program https://studentprivacy.ed.gov/resources/case-study-2-head-start-program
- Case Study #3: Enforcement https://studentprivacy.ed.gov/resources/case-study-3-enforcement

- Case Study #4: PTAC Technical Assistance https://studentprivacy.ed.gov/resources/case-study-4-ptac-technical-assistance
- Case Study #5: Minimizing Access to PII https://studentprivacy.ed.gov/resources/case-study-5-minimizing-pii-access
- Joint Guidance on Data Matching to Facilitate WIOA Performance Reporting and Evaluation https://studentprivacy.ed.gov/resources/joint-guidance-data-matching-facilitate-wioa-performance-reporting-and-evaluation
- Joint Guidance on the Application of the Family Educational Rights and Privacy Act (FERPA) And the Health Insurance Portability and Accountability Act of 1996 (HIPAA) To Student Health Records https://studentprivacy.ed.gov/resources/joint-guidance-application-ferpa-and-hipaa-student-health-records
- Guidance on the Amendments to the Family Educational Rights and Privacy Act by the Uninterrupted Scholars Act https://studentprivacy.ed.gov/resources/uninterrupted-scholars-act-guidance
- Technical Assistance on Student Privacy for State and Local Educational Agencies When Administering College Admissions Examinations https://studentprivacy.ed.gov/admissions-exams
- Disclosure Avoidance https://studentprivacy.ed.gov/resources/frequently-asked-questions-disclosure-avoidance
- Data De-Identification Basic Terms: https://studentprivacy.ed.gov/resources/data-de-identification-overview-basic-terms
- OSPI Suppression Rules for Public Reporting https://k12.wa.us/sites/default/files/public/StudentInformation/SuppressionRulesforPublicReporting.pdf
- Technical Assistance on Student Privacy for State and Local Educational Agencies When Administering College Admissions Examinations: https://studentprivacy.ed.gov/admissions-exams
- Uninterrupted Scholars Act Guidance https://www2.ed.gov/policy/gen/guid/fpco/ferpa/uninterrupted-scholars-act-guidance.pdf
- PTAC FERPA Exemptions Handout https://studentprivacy.ed.gov/sites/default/files/resource_document/file/FERPA%20Exceptions_HANDOUT_horizontal_0.pdf
- National Association of Student Financial Aid Administrators, Financial Aid Data Sharing Report (Version 2), 2019 https://www.nasfaa.org/uploads/documents/June_2019_Data_Sharing_White_Paper.pdf

Compliance with State Laws & Guidelines

In addition to complying with federal regulations, ERDC is responsible for meeting the requirements of Washington state law. An essential law that governs ERDC's work is RCW 43.41.400, the legislation that enabled the creation of the ERDC and directs the work of the ERDC.

RCW 43.41.400

(1) An education data center shall be established in the office of financial management. The education data center shall jointly, with the legislative evaluation and accountability program committee, conduct collaborative analyses of early learning, K-12, and higher education programs and education issues across the P-20 system, which includes the department of children, youth, and families, the superintendent of public instruction, the professional educator standards board, the state board of education, the state board for community and technical colleges, the workforce training and education coordinating board, the student achievement council, public and private nonprofit four-year institutions of higher education, and the employment security department. The education data center shall conduct collaborative analyses under this section with the legislative evaluation and accountability program committee and provide data electronically to the legislative evaluation and accountability program committee, to the extent permitted by state and federal confidentiality requirements. The education data center shall be considered an authorized representative of the state educational agencies in this section under applicable federal and state statutes for purposes of accessing and compiling student record data for research purposes.

(2) The education data center shall:

(a) In consultation with the legislative evaluation and accountability program committee and the agencies and organizations participating in the education data center, identify the critical research and policy questions that are intended to be addressed by the education data center and the data needed to address the questions;

(b) Coordinate with other state education agencies to compile and analyze education data, including data on student demographics that is disaggregated by distinct ethnic categories within racial subgroups, and complete P-20 research projects;

(c) Collaborate with the legislative evaluation and accountability program committee and the education and fiscal committees of the legislature in identifying the data to be compiled and analyzed to ensure that legislative interests are served;

(d) Annually provide to the K-12 data governance group a list of data elements and data quality improvements that are necessary to answer the research and policy questions identified by the education data center and have been identified by the legislative committees in (c) of this subsection. Within three months of receiving the list, the K-12 data governance group shall develop and transmit to the education data center a feasibility analysis of obtaining or improving the data, including the steps required, estimated time frame, and the financial and other resources that would be required. Based on the analysis, the education data center shall submit, if necessary, a recommendation to the legislature regarding any statutory changes or resources that would be needed to collect or improve the data;

(e) Monitor and evaluate the education data collection systems of the organizations and agencies represented in the education data center ensuring that data systems are flexible, able to adapt to evolving

needs for information, and to the extent feasible and necessary, include data that are needed to conduct the analyses and provide answers to the research and policy questions identified in (a) of this subsection;

(f) Track enrollment and outcomes through the public centralized higher education enrollment system;

(g) Assist other state educational agencies' collaborative efforts to develop a long-range enrollment plan for higher education including estimates to meet demographic and workforce needs;

(h) Provide research that focuses on student transitions within and among the early learning, K-12, and higher education sectors in the P-20 system;

(i) Prepare an annual report on the educational and workforce outcomes of youth in and released from institutional education facilities as defined in RCW 28A.190.005, using data disaggregated by age, and by ethnic categories and racial subgroups in accordance with RCW 28A.300.042. The annual report required by this subsection (2)(i) must be provided to the office of the superintendent of public instruction in a manner that is suitable for compliance with RCW 28A.190.110; and

(j) Make recommendations to the legislature as necessary to help ensure the goals and objectives of this section and RCW 28A.655.210 and 28A.300.507 are met.

(3) The department of children, youth, and families, superintendent of public instruction, professional educator standards board, state board of education, state board for community and technical colleges, workforce training and education coordinating board, student achievement council, public four-year institutions of higher education, department of social and health services, and employment security department shall work with the education data center to develop data-sharing and research agreements, consistent with applicable security and confidentiality requirements, to facilitate the work of the center. The education data center shall also develop data-sharing and research agreements with the administrative office of the courts to conduct research on educational and workforce outcomes using data maintained under RCW 13.50.010(12) related to juveniles. Private, nonprofit institutions of higher education that provide programs of education beyond the high school level leading at least to the baccalaureate degree and are accredited by the Northwest association of schools and colleges or their peer accreditation bodies may also develop data-sharing and research agreements with the education data center, consistent with applicable security and confidentiality requirements. The education data center shall make data from collaborative analyses available to the education agencies and institutions that contribute data to the education data center to the extent allowed by federal and state security and confidentiality requirements applicable to the data of each contributing agency or institution.

Additional ERDC State Reporting Requirements

Several state statutes specifically require ERDC to produce reports for the legislature or work groups. Additionally, some state statutes require ERDC to collect or share data with other state agencies or research groups (like JLARC, LEAP, or WSIPP) for required reports for the legislature. A detailed list of current state reporting requirements can be found on our website.

OCIO Data Categories

Office of the Chief Information Officer (OCIO) Policy 141.10 Securing Information Technology Assets, Standard 4.1 Data Classification requires that agencies "must classify data into categories based on the sensitivity of the data." Additionally, Agency data classifications must translate into or include 4 categories identified by the OCIO. Under 141.10, 4.2 Data Sharing, when sharing Category 3 or 4 data outside the agency an agreement must be in place unless otherwise prescribed by law. The agreement must, among other things include the categorization of the data.

The Division, in coordination with OFM Legal and Legislative Affairs' contracts unit, prepares P20W Data Sharing Agreements and Data Use Agreements. Data Classification Agencies must classify data into categories based on the sensitivity of the data. Agency data classifications must translate to or include the following classification categories:

(1) Category 1 – Public Information

Public information is information that can be or currently is released to the public. It does not need protection from unauthorized disclosure, but does need integrity and availability protection controls.

(2) Category 2 – Sensitive Information

Sensitive information may not be specifically protected from disclosure by law and is for official use only. Sensitive information is generally not released to the public unless specifically requested.

(3) Category 3 – Confidential Information

Confidential information is information that is specifically protected from either release or disclosure by law. This includes but is not limited to: a. Personal information as defined in RCW 42.56.590 and RCW 19.255.10. b. Information about public employees as defined in RCW 42.56.250. c. Lists of individuals for commercial purposes as defined in RCW 42.56.070 (9). d. Information about the infrastructure and security of computer and telecommunication networks as defined in RCW 42.56.420.

(4) Category 4 – Confidential Information Requiring Special Handling

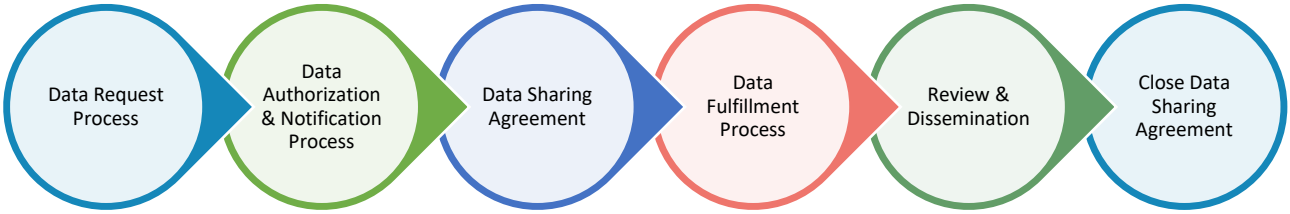
Confidential information requiring special handling is information that is specifically protected from disclosure by law and for which: a. Especially strict handling requirements are dictated, such as by statutes, regulations, or agreements. b. Serious consequences could arise from unauthorized disclosure, such as threats to health and safety, or legal sanctions.

OCIO also provides guidance regarding Data Sharing Agreements (see below).

Detailed P20W Business Processes: External Data Requests

State agencies, academic researchers from schools and universities, and external research groups can request data from ERDC. ERDC staff members are available to consult with requestors about data availability, quality, and cohort design. ERDC also produces several products intended to support data requestors through this process: https://erdc.wa.gov/data-resources/working-erdc-data.

Figure 4. Overview of the process for external parties to access ERDC data



ERDC Data Request Process

All requestors, regardless of their role or agency must follow this request process:

1. Plan your data request

Be prepared to tell the ERDC about your research questions, the purpose of the project, funding, study population, variables requested, which education sectors data will come from, and your research methodology. If you plan to request individual-level data, you may need to receive approval from our data contributors. Be prepared to contact them and answer questions about your data request, including your research questions and variables needed.

2. Determine your data type

Understanding the type of data that you need is key to your data request process. The ERDC strongly encourages aggregate data requests, both to limit the amount of individual-level data shared and to expedite your data request. In cases where individual-level data is necessary, the ERDC will work with you to gain approval from data contributors, create a data-sharing agreement, and will require a review of any future publications using that data. See the Key Terms section of this document for definitions of terms.

OFM can fulfill data under three data types: 1) redacted aggregate data, 2) unredacted aggregate or 3) individual level data requests. OFM does not redisclose any direct identifiers.

1) **Redacted Aggregate Data Requests.** *Redacted aggregate data* does not reveal any student's personal information, either directly or in combination with other available information. This is typically summary data that does not allow someone to learn information about a specific

student. This data can be shared without a data-use agreement, as it doesn't violate FERPA standards. OFM may anonymize and/or aggregate subsets of such Personally Identifiable Information (PII) for the minimum disclosure needed to satisfy a request of a third-party engaging in research on cross-sector or cross-institution topics. Before redisclosure, the OFM will ensure that PII is sufficiently anonymized and/or aggregated such that the resulting information no longer identifies a specific student. This includes the reidentification of the resulting information is impossible including, but not limited to, by combination or association with any other information independently in the possession of a third-party data requestor.

2) **Unredacted Aggregate Data Requests.** *Unredacted aggregate data* may allow individuals to be identified. Such data is protected by FERPA and other privacy laws. To prevent sharing personal information, the ERDC either excludes numbers from summary tables (suppression of information where the total number of students is less than 10) or requires a data-use agreement under FERPA. OFM may provide aggregate data tables where a limited number of cells fall below redisclosure requirements. Prior to the redisclosure of data for these types of requests, OFM will: Ensure that each redisclosure to a Data Requestor shall be permitted under and complies with FERPA; Only redisclose the minimum possible data for it and/or a Data Requestor to comply with applicable law; and confirm the request has received Institutional Review Board approval (if necessary for the study).

3) **Individual Level Data Requests.** Individual-level data may include indirect identifiers, but no direct identifiers of student data. Prior to the redisclosure of data for these types of requests, OFM will: Ensure that each redisclosure to a Data Requestor shall be permitted under and complies with FERPA; Only redisclose the minimum possible data for it and/or a Data Requestor to comply with applicable law; and confirm the request has received Institutional Review Board approval (if necessary for the study).

3. Complete a data request form

Once you have determined your data type, complete the appropriate form (see ERDC website for most current forms). If you are requesting individual data or unredacted aggregate data, then you must submit both the Individual Data Request Form and the Individual Data Table to ERDC.

4. Submit your request to the ERDC

Email your data request to erdc@ofm.wa.gov.

Please allow up to a week for an initial response. The time it takes to review and fulfill a request depends on the complexity of the data.

When ERDC has received a data request, that kicks off the **Data Authorization Process.**

Data Authorization Process

1. Data request received in ERDC inbox.

The Data Governance Coordinator (DGC) saves the data request form and assigns the request a request or "R" number (ex. R5123). At this point, the DGC also does an initial review and logs the request in SharePoint. If there are any key pieces of information, the DGC may reach out for clarification or for submittal of a new form.

2. Data request reviewed by ERDC Staff Members

The Data Governance Coordinator, Data Warehouse Manager, and ERDC Director coordinate to answer the following questions:

1. Does ERDC have jurisdiction to process the request?
2. Does the request fall under an allowable FERPA exception for redisclosure?
3. Does the DSA with the data contributor(s) authorize this request/use of the data?
4. Are the minimum data elements to answer the research questions being requested?
5. Does the request need IRB approval?
6. Can the requester meet our data security standards or sign up for Enclave accounts?
7. Is this request feasible for ERDC to fulfill with data currently available in the timeline requested?
8. Does ERDC have the current staff capacity to support this request?
9. Is the request aligned with ERDC's research agenda?

If the request meets all the above requirements, it is then passed onto the data contributors for review (See Figure 5). Depending on the data contributor, authorization may not be necessary per the data sharing agreement with ERDC. For those contributors, notification is provided. See Table 2 below for an overview of which contributors require authorization and which require notification.

Table 2. Overview of authorization or notification process as determined by data contributor DSA's

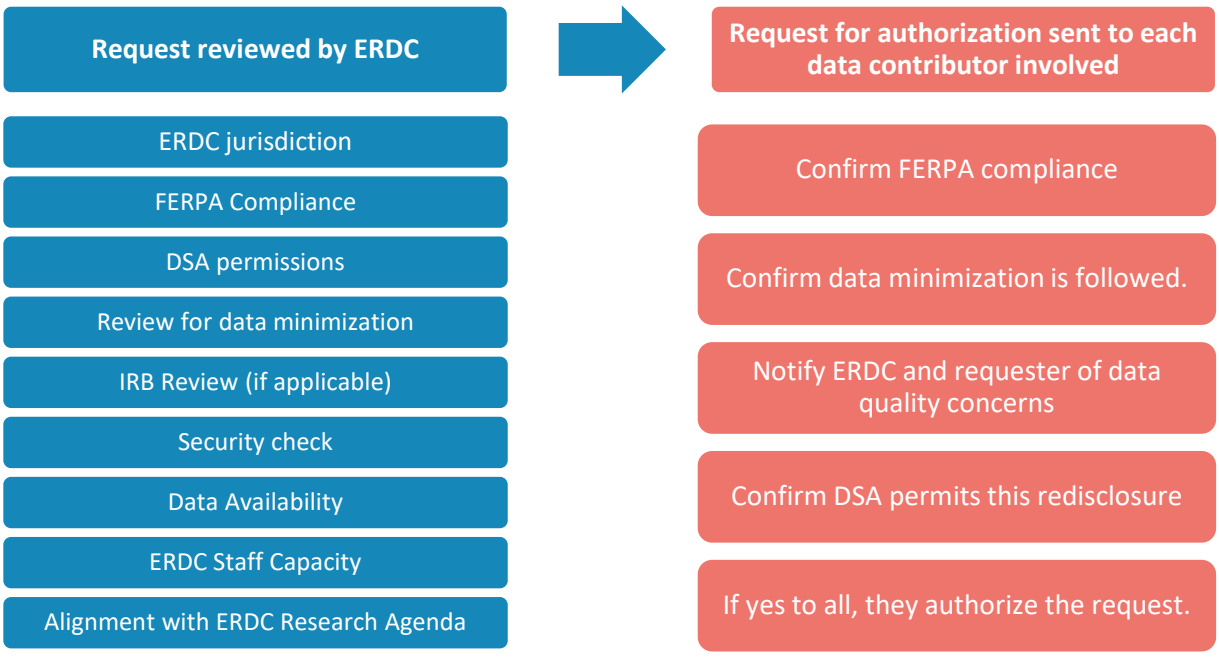
Agency	Authorization or Notification?
Administrative Office of The Courts	Written authorization to designate requestor as an authorized representative of the agency
Public Four-Year Universities (PCHEES)	OFM can designate requestor as an authorized representative per DSA; notification required
Department of Children, Youth & Families	Written authorization to designate requestor as an authorized representative of the agency
Department of Corrections	Written authorization to designate requestor as an authorized representative of the agency
Educator Prep Programs (EPP)	Written authorization to designate requestor as an authorized representative of the agency
Employment Security Department	Written authorization to designate requestor as an authorized representative of the agency
Office of Superintendent of Public Instruction	Written authorization to designate requestor as an authorized representative of the agency

Agency	Authorization or Notification?
State Board Community & Technical Colleges	OFM can designate requestor as an authorized representative per DSA; notification required
Labor & Industries	OFM can designate requestor as an authorized representative per DSA; notification required
Workforce Training Board (WTB)	OFM can designate requestor as an authorized representative per DSA; notification required
Washington Student Achievement Council	Written authorization to designate requestor as an authorized representative of the agency

3. Designation of Requester as an Authorized Representative

For data sharing agreements where a written authorization to designate the data requestors as an authorized representative of the contributing agency is required, ERDC sends the data contributor the Data Request Form and the Individual Level Data Table for review. The data contributor checks for the items listed in Figure 5. If it is satisfactory, the data contributor completes the Data Authorization Form. This form is emailed back to the ERDC Data Governance Coordinator, typically within two weeks. If there are follow-up questions or concerns, the ERDC helps to facilitate conversations between the requestor and the data contributor. However, the final determination of whether ERDC can share the data is up to the data contributor(s).

Figure 5. Outline of standard questions that are part of the review and authorization process:



4. Notification

In two current data sharing agreements (SBCTC and L&I) ERDC and the data contributor have agreed that ERDC does not need to seek authorization for data requests. In these instances, ERDC will notify the data

contributor of the request and subsequent release of data, regardless of whether it is redacted aggregate data, unredacted aggregate data, or individual level data.

5. Authorizations Received

When the authorization process is complete, the data request moves to the **Data Sharing Agreement Process.**

Frequently Asked Questions about Accessing ERDC Data

Does my project require data linked from multiple agencies (cross-sector data)?

ERDC receives and links data from multiple sources, including early childhood education, K-12, WA public 4-year and 2 year postsecondary and employment sectors (cross-sector). ERDC can't fulfill requests for data from a single sector- only multiple. To request data from a single sector, contact the data provider. Not sure if your request is for in-sector or cross-sector data? Contact the ERDC.

Is my request for (a) individual-level data or unredacted aggregate data or (b) redacted aggregate data?

Requests for individual-level data (including de-identified or identifiable data) or unredacted aggregate data require an extensive review involving FERPA compliance, WSIRB review, and data use agreements. Requests for redacted aggregate data have fewer requirements and represent less risk. ERDC prefers sharing redacted aggregate data to minimize disclosures and risk.

Is my request compliant with the Family Educational Rights and Privacy Act?

FERPA safeguards the confidentiality of individual student information. That's why ERDC will consider the following when they review your request:

Does your request fall under a FERPA exception?

The most common exceptions for ERDC cross-sector data are 1) the audit and evaluation exception or 2) the studies exception.

Does your request relate to an education program?

FERPA defines an education program as "any program that is principally engaged in the provision of education, including, but not limited to, early childhood education, elementary and secondary education, postsecondary education, special education, job training, career and technical education, adult education, and any program that is administered by an educational agency or institution."

Does the Washington State IRB need to review my project?

Depending on your research questions and design, your study may need to undergo a Washington State Institutional Review Board review. Upon request, the ERDC can consult with you about what type of review your request might require. Requests typically fall into three categories: a full IRB review, an

expedited review, or exempt review.

Can my agency sign a data sharing agreement?

If there is not a data sharing agreement in place, ERDC will create a data sharing agreement with the data requester. Key components of this agreement include data privacy, constraints on how you can use the data, data security, and data destruction.

Role of IRB

The WSIRB is a designated institutional review board (IRB) for different Washington state agencies, including the Washington State Departments of Children, Youth, and Families (DCYF), Health (DOH), Corrections (DOC), Social and Health Services (DSHS), Health Care Authority (HCA), Labor & Industries (L&I), and the Office of Financial Management (OFM).

As part of the data approval process, ERDC determines whether the project request needs to have IRB approval prior to sharing any data. ERDC staff consider the following questions, in consultation with the researcher and WSIRB staff.

Does the proposed project meet the federal and state agency definition of research?

According to the Washington State Institutional Review Board (WSIRB), "research" means a systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalizable knowledge. Activities that meet this definition constitute research, whether they are conducted or supported under a program which is considered research for other purposes.

Systematic investigation. A detailed or careful examination that has or involves a prospectively identified approach to the activity based on a system, method, or plan.

Generalizable knowledge. Information is expected to expand the knowledge base of a scientific discipline or other scholarly field of study and yield one or both of the following:

- Results that are applicable to a larger population beyond the site of data collection or the specific subjects studied.
- Results that are intended to be used to develop, test, or support theories, principles, and statements of relationships, or to inform policy beyond the study.

According to the WSIRB, some activities resemble research but actually are not research as defined in the federal regulations and state agency policy. Program evaluation, surveillance, disease investigation, and quality assurance and/or quality improvement are activities that may or may not constitute research that requires WSIRB review.

If the request meets the definition of research, then the data requestor/researcher is expected to submit an IRB application to the WSIRB. Visit the IRB website for relevant forms and the fee structure. Data will only be shared after ERDC receives a copy of the letter of approval or exemption from the WSIRB (or an IRB that has an IRB Authorization Agreement with WSIRB, see below).

If the request does not meet the definition of research, it does not need IRB approval for the data request to be fulfilled.

What if the researcher obtained prior authorization from a different IRB?

The WSIRB has established multiple project IRB Authorization Agreements with the University of Washington, Eastern Washington University, Washington State University, other state agencies and other institutions. These Agreements allow one institution to rely on the IRB review of another institution. If you are affiliated with any of these institutions, review the relevant IRB Authorization Agreement and/or check with the IRB of your home institution to determine whether they will rely on the WSIRB for the review of your research.

If you are have any questions about IRB, please visit their website at https://www.dshs.wa.gov/ffa/human-research-review-section or contact IRB directly at wsirb@dshs.wa.gov

Data Sharing Agreement Process

After an external request for individual level or unredacted aggregate has been approved by data contributors and before it can be fulfilled, the ERDC must establish a data sharing agreement with the data requestor. The ERDC is supported by the OFM contracts staff to guide this request. For more about data sharing agreements and best practices refer to the FERPA Guidance for Reasonable Methods and Written Agreements. The Office of Privacy and Data Protection within the Office of the Chief Information Officer has also created Data Sharing Agreement Implementation Guidance. When the data sharing agreement has a been executed, the data request moves to the **Data Fulfillment Process.**

1. OFM determines method for delivery of data

OFM can deliver data using an MFTP account or can house the data in the ERDC Education Data Enclave. Choosing the method of delivery informs what type of protections and requirements need to be applied in the data sharing agreement.

2. OFM drafts agreement using the appropriate DSA template

The ERDC Data Governance Coordinator drafts an agreement using the template and the data request form submitted by the researcher. The data request form typically includes information about the scope, timeline, research questions, and specifies the data elements that are being requested. It also details the cohort and years of data requested. All this information is included in the agreement.

3. OFM sends draft to data requestor for review and clarifies any missing information

If necessary, OFM seeks clarification on any items missing in the DSA not covered on the data request form and asks for the DSA administrator and privacy administrator of the requesting agency.

4. Requesting agency reviews and notifies OFM if they have concerns or if they are ready to sign.

Once the requesting agency has reviewed and agrees with the terms of the DSA, the OFM Information Technology contracts staff sends them an electronic copy for signatures via DocuSign.

5. NDA Forms

OFM will also send via DocuSign NDA forms for any individuals at the requesting agency that access the data through the analysis or review process. The requesting agency must notify ERDC if there are changes to staff who access the data.

Requirements for Data Sharing Agreements

Office of Privacy and Data Protection (OPDP) provides guidance and outlines requirements for state data sharing agreements. All OFM contracts are reviewed by the ERDC Data Governance Coordinator, the ERDC Director, the Forecasting & Research Assistant Director, and then submitted to the OFM contracts for additional review and edits to ensure that the contract meets state and federal requirements and best practices.

The following is an excerpt from the Data Sharing Agreement Implementation Guidance (December, 2021) created by the Office of Privacy and Data Protection (OPDP):

"Data Sharing Agreement Requirements Broad DSA requirements (in addition to requirements that may apply to specific agencies or specific types of information) exist for Washington state agencies in at least three places:

> RCW 39.26.340(1) states that "[b]efore an agency shares with a contractor category 3 or higher data, as defined in policy established in accordance with RCW 43.105.54, a written data-sharing agreement must be place." Within chapter 39.26 RCW, agency means office or activity of the executive or judicial branches of state government.
>
> RCW 39.34.240(1) states that "[i]f a public agency is requesting from another public agency category 3 or higher data . . . the requesting agency shall provide for a written agreement between the agencies . . . ." Within chapter 39.34 RCW, a public agency means any agency, political subdivision, or unit of local government; any state agency; any United States agency; any federally recognized tribe; and any political subdivision of another state.
>
> OCIO Policy #141.10 states that "[w]hen sharing Category 3 and above data outside the agency, an agreement must be in place unless otherwise prescribed by law." OCIO Policy #141.10 applies to executive branch agencies and agencies headed by separately elected officials.

Taken individually these requirements could conceivably be interpreted to create a patchwork of DSA mandates. But together they reinforce the best practice that an agency should typically enter DSAs when a person outside the agency receives or has access to confidential information. Entering into DSAs is also consistent with the Washington State Agency Privacy Principles. It is most obviously a core part of the due diligence principle, which requires exercising care when sharing information with third parties. DSAs also support the remaining principles by carrying forward the agency's own obligations as a trusted steward of information and are one part of ensuring an agency understands all the places where its data is located."

Mandatory Clauses in Data Sharing Agreements

In addition to data sharing agreements outlined by OPDP, OFM's Redisclosure data sharing agreement for FERPA regulated data will include the following mandatory clauses, depending on which exception the data is provided under. Data Sharing Agreements between OFM and the Data Requestor will include the terms required by FERPA, as stated below.

Redisclosure Data Sharing Agreements from OFM will also include:

1. A survivorship clause relating to the DSA data breach clause;
2. The same level of protection for Institutional Data as required by the incoming DSA; and
3. A prohibition on further redisclosure or re-identification by the Data Requestor except as required by law.

Studies Exception

The FERPA regulations on the studies exception requires that the educational agency or institution or the state or local education authority or agency headed by an official listed in 34 CFR §99.31(a)(3) execute a written agreement with the organization conducting the study when disclosing personally identifiable information from education records without consent (see 34 CFR §99.31(a)(6)(iii)(C)).

Written agreements under the studies exception will be in accordance with the requirements in §99.31(a)(6)(iii)(C), which currently requires the following:

1. Specify the purpose, scope, and duration of the study and the information to be disclosed.
2. Require the organization to use personally identifiable information (PII) from education records only to meet the purpose or purposes of the study as stated in the written agreement.
3. Require the organization to conduct the study in a manner that does not permit the personal identification of parents and students by anyone other than representatives of the organization with legitimate interests. This typically means that the organization should allow internal access to PII from education records only to individuals with a need to know, and that the organization should take steps to maintain the confidentiality of the PII from education records at all stages of the study, including within the final report, by using appropriate disclosure avoidance techniques.
4. Require the organization to destroy all PII from education records when the information is no longer needed for the purposes for which the study was conducted and specify the time period in which the information must be destroyed.

Audit or Evaluation Exception

The FERPA regulations on the audit or evaluation exception require that the state or local education authority or agency headed by an official listed in 34 CFR §99.31(a)(3) must use a written agreement to designate any authorized representative other than an employee (see 34 CFR §99.35(a)(3)).

The current version of Section 99.35(a)(3) of FERPA specifically requires that the following provisions be included in written agreements under the audit or evaluation exception:

1. Designate the individual or entity as an authorized representative and formally designate the individual or entity as an authorized representative.
2. Specify the PII from education records to be disclosed.
3. Specify that the purpose for which the PII from education records is being disclosed to the authorized representative is to carry out an audit or evaluation of Federal- or state-supported education programs, or to enforce or to comply with Federal legal requirements that relate to those programs. The agreement will state specifically that the disclosure of the PII from education records is in furtherance of an audit, evaluation, or enforcement or compliance activity.
4. Describe the activity with sufficient specificity to make clear that it falls within the audit or evaluation exception. This must include a description of how the PII from education records will be used. The agreement will describe in detail the methodology and why

disclosure of PII from education records is necessary to accomplish the audit, evaluation, or enforcement or compliance activity.

5. Require the authorized representative to destroy the PII from education records when the information is no longer needed for the purpose specified.
6. Specify the time period in which the PII must be destroyed.
7. Establish policies and procedures, consistent with FERPA and other Federal and state confidentiality and privacy provisions, to protect PII from education records from further disclosure (except back to the disclosing entity) and unauthorized use, including limiting use of PII from education records to only authorized representatives with legitimate interests in an audit, evaluation, or enforcement or compliance activity. The agreement must establish the policies and procedures, consistent with FERPA and other Federal and state laws, to protect PII from education records from further disclosure or unauthorized use.

What if misconduct occurs?

If data requesters breach their contract/DSA with ERDC and misuse the data, for example by re-identifying records or not adequately suppressing small cell counts, ERDC will follow processes that are outlined in the Data Sharing Agreement.

ERDC DSA Extension Steps

As an agreement nears expiration, the follow process takes place:

1. The Data Governance Coordinator (DGC) receives automated email from ECMS 3 months prior to DSA expiration reminding the DGC that a DSA will be ending.

2. DGC sends a reminder email to the data request DSA administrator about upcoming expiration.

   The email may include the following types of questions:

   a. Need to extend? For how long?
      i. If no, proceed to Closing out Data Sharing Agreements.
   b. Reminder to delete the data and send the completed data destruction form on or prior to expiration
   c. If no products have been received, requests the data products
   d. Place email in project folder

3. If extending, DGC drafts an amendment to the DSA and sends to the DSA administrator or data requestor for review.

4. Once the amendment language is agreed upon, DGC sends contract amendment to the DSA administrator via the OFM Information Technology contracts DocuSign account.

   DR sends signed contract amendment back via DocuSign and then the OFM Contracts office signs. ERDC inbox automatically receives copies of signed amendment. The OFM Contracts Office updates ECMS and sends copy of signed contract amendment to DGC.

Data Fulfillment Process

Data fulfillment includes people processes, technical safeguards, as well as disclosure limitation methods.

Accessing ERDC Data

Once the data sharing agreement has been executed and the data request has been fulfilled, there are two possible ways that the data requestor may receive the data.

Education Data Enclave

A data enclave is a secured virtual desktop environment that researchers can use to access data, conduct analyses, and create research products – all in one remote workspace. Data enclaves are popular tools used by academic and applied research organizations across the country. The ERDC contracts with NORC at the University of Chicago to provide a data enclave for ERDC data requesters to use for research purposes. The ERDC's Education Data Enclave (EDE) enables researchers to analyze requested record-level data remotely with software and data visualization tools that are costly to purchase on their own. The EDE is the ERDC's preferred approach to fulfill requests for record-level data.

Read more about the data enclave here.

MFT Accounts

In situations where the ERDC determines that the enclave is not an appropriate solution to deliver data, an MFT account will be created for the data requestor to access the data.

Review and Dissemination

Protecting student privacy and ensuring that data is used with integrity and accuracy extends into the dissemination of research products that involve ERDC data. In our data sharing agreements with data requestors, ERDC stipulates the following:

Statement for Publications

To the extent, if any, that the data will be shared by the Requestor with entities other than OFM, the Requestor shall include the following statement:

"The research presented here uses confidential data from the Education Research and Data Center (ERDC) located within the Washington Office of Financial Management (OFM). ERDC's data system is a statewide longitudinal data system that includes de-identified data about people's preschool, educational, and workforce experiences. The views expressed here are those of the authors and do not necessarily represent those of OFM or other data contributors. Any errors are attributable to the authors."

Suppression Requirements

Recipient will follow applicable federal and state laws protecting student and employment data, and the guidelines specified in the Institute of Education Sciences SLDS Technical Brief, Statistical Methods for Protecting Personally Identifiable Information in Aggregate Reporting (NCES 2011-603 https://nces.ed.gov/pubsearch/pubsinfo.asp?pubid=2011603) when displaying student information in

public reports. Publicly-reported aggregated results will not contain any group of fewer than 10 individuals adopting RCW 28A.544.090 as the standard.

When displaying employment data, Recipient must ensure that cell sizes are ample enough so that one record does not contain 80% of the wages or hours of a particular reporting cell. Other considerations when using employment data can be found in ERDC Technical Report 2012-01, Employment Data Handbook located at https://erdc.wa.gov/technical-resources.

Review Requirements

Recipient must provide draft report(s) to OFM and data contributors at least ten (10) working days prior to any public release of reports to verify proper disclosure avoidance techniques have been used and communicate with OFM or data contributors when questions arise regarding data provided.

At the conclusion of the project, the requester is asked to provide ERDC with any public reports or publications, including dashboards, that were created using ERDC data (including weblinks). These are posted on ERDC's website to demonstrate the use of ERDC data.

Closing out Data Sharing Agreements

1. Check for extension.

The DGC makes sure that the data requestor does not want to extend the DSA following the process outlined in the data sharing agreement process above.

2. Request for Data Destruction Form

Upon expiration, if completed and signed Data Destruction Form has not yet been received, DGC sends DR DSA administrator an email requesting it again and save email in project folder

3. Request for any related data products

Upon expiration, if data product has not been received, send another email request for the data product and save email in project folder

4. Store Data Destruction Form

When the completed and signed Data Destruction Form has been received DCG places in project folder and upload to ECMS (via OFM Contracts staff). If any associated data products are received, DCG places data product in project folder.

5. Delete associated accounts and data

DGC sends request to the DMW to delete MFT account or the enclave account. DGC requests DWM to delete external match data set, if applicable

Internal ERDC Data Access

ERDC data scientists and researchers access the P20W data to meet our statutory obligations to compile and analyze education data, as well as provide analysis and research across the P20W education system in response to grant requirements, data requests, and to address topics identified under our critical questions.

No data sharing agreement is created because there is no redisclosure of the data beyond ERDERDC will provide updates on internal OFM research activities through quarterly reporting to data contributors and updates at governance committee meetings.

Internal Review

Suppression. ERDC researchers follow applicable federal and state laws protecting student and employment data, and the guidelines specified in the Institute of Education Sciences SLDS Technical Brief, Statistical Methods for Protecting Personally Identifiable Information in Aggregate Reporting (NCES 2011-603 https://nces.ed.gov/pubsearch/pubsinfo.asp?pubid=2011603) when displaying student information in public reports. Publicly-reported aggregated results will not contain any group of fewer than 10 individuals.

When displaying employment data, OFM/ERDC researchers must ensure that cell sizes are ample enough so that one record does not contain 80% of the wages or hours of a particular reporting cell.

Internal Review. OFM/ERDC has an internal review process for all ERDC research publications. While each publication may have special considerations, the overall format of the review process includes:

1. Internal Review - Each publication is reviewed for the following - (1) Data and Methods; (2) Governance; (3) Content.
2. External Review – Project partners and data contributors will each be provided draft publications at least ten (10) working days prior to any public release of reports to verify proper disclosure avoidance techniques were used.
3. Communications Review - Research report is sent to OFM communications for copy editing and to ensure the structure and content adhere to OFM writing guidelines, including accessibility of figures with a screen reader.
4. Publication - Publication is posted on ERDC website and released via the ERDC newsletter subscription list.

P20W People Roles: ERDC Personnel

ERDC Role Definitions related to Data Governance

- Assistant Director of OFM Forecasting & Research- Oversees OFM Forecasting & Research, including the ERDC

- ERDC Director – Supervises the staff and provides strategic direction for the ERDC; oversees all processes related to governance and research.

- Senior Data Governance and Operations Specialist (DGC) - Responsible for the data request review process, the data authorization and approval process, the data sharing agreement process, and closure of data sharing agreements. Works with the DWM in preparing for the data fulfillment process.

- Senior Research Scientist- Responsible for conducting research and overseeing the design and methodology used across all ERDC research activities

- Data Contributor – An organization that provides ERDC with data to for feeding into the P20W data system

- Data Warehouse Manager (DWM) - Responsible for the day-to-day operations related to data management activities for P20W data.

- Data Requestor – A non ERDC member requesting a dataset involving cross-sector data

- Data Steward - The main point of contact between the data provider and the ERDC. Acts as a resource for staff researchers on sector-specific data questions, coordinates data transfers with provider, and performs data profiling of source data

- Senior Data Operations Specialist: Helps document tasks, timing, and requirements around ongoing P20W data sources and system enhancements. Oversees data steward activities.

- Research Scientist - ERDC or grant staff that are responsible for designing study and performing activities necessary to fulfill research requirements

- Senior Data Scientist- Responsible for data request fulfillment, including the handling of confidential information and using disclosure limitation methods.

- OFM Privacy Officer – The Privacy Officer provides oversight of the OFM Privacy Program under Executive Order 16-01, Privacy Protection and Transparency in State Government, and confidentiality regulations. Oversees the OFM Information Technology contracts and data sharing agreements.

- OFM Chief Security Officer- The Chief Information Security Officer (CISO) addresses information technology security issues. The CISO also supports the privacy officer in administering the OFM Privacy Program.

Data access for ERDC and OFM staff

OFM Policy

The Office of Financial Management policy 4.02 pertains to Handling OFM information. The purpose of this policy is to reduce the risk of mishandling information held by the Office of Financial Management, with a focus on confidential information, and to reduce the risk for unauthorized access, disclosure,

sharing, use, and destruction of information held by OFM. This policy establishes the requirement for signing OFM employee non-disclosure agreements (NDA), provides the process to obtain a signed NDA from OFM employees, and states the consequences of violating the NDA. This policy is to ensure that employees understand:

- the access and use of information are for official business purposes only, and
- other requirements and restrictions related to access and sharing of information.

All employees must sign an Office of Financial Management non-disclosure agreement, which details expectations for employee access and use of all information. Additionally, an NDA, also called a confidentiality agreement, may be required for specific information or category of data (for example, medical data or student records) based on statutory or regulatory requirements governing the specific type of data.

OCIO Policy

Office of the Chief Information Officer (OCIO) Policy 141.10 Securing Information Technology Assets, Standard 4.1 Data Classification requires that, "Data Sharing Agencies must ensure that sharing data with the public at large complies with the OCIO Public Records Privacy Protection Policy and other applicable statutes or regulations." When sharing Category 3 and above data outside the agency, an agreement must be in place unless otherwise prescribed by law. The agreement (such as a contract, a service level agreement, or a dedicated data sharing agreement) must address the following: (1) The data that will be shared. (2) The specific authority for sharing the data. (3) The classification of the data shared. (4) Access methods for the shared data. (5) Authorized users and operations permitted. (6) Protection of the data in transport and at rest. (7) Storage and disposal of data no longer required. (8) Backup requirements for the data if applicable. (9) Other applicable data handling requirements.

Additional ERDC limitations on data access for staff

Data access is limited to the staff members that are responsible for the maintenance of the data or those that are conducting research that involves the data. In both instances, the ERDC staff member signs any relevant nondisclosure agreements from the data contributor(s). Individuals that review data products, including dashboards or research reports, are also required to sign an NDA to view the analyses and reports prior to publication.

More information about technical structures to limit data access can be found in the Data Security Manual.

Data Governance Training for ERDC Staff

CITI Program

ERDC research staff are required to complete the CITI Program Human Subjects Research Training.

Learn more here: https://about.citiprogram.org/series/human-subjects-research-hsr/?h=human%20subjects%20research

The Data Governance Coordinator is responsible for tracking these trainings to make sure all ERDC staff are up to date.

OFM Training

In addition to numerous other options, these trainings are required and available through OFM's intranet site:

WA State IT Security Awareness Training – all employees – frequency = once

This course covers IT security issues and tests employees understanding and treatment of different types of security risks.

Privacy Basics for Washington State Employees – all employees – frequency = every two years

This course provides an overview of personal information, data categorization, and privacy harms and violations in addition to the privacy laws of Washington state and the OFM privacy principles.

Records 101 – all employees – frequency = once

This course covers the management and disclosure of public records, including relevant statutes, rules and policies applicable to all agency employees.

Records Management 102 – all employees – frequency = every 3 years

This course refreshes information previously provided in OFM Records Management 101, covering basic records topics and various statutes and policies related to managing records as a public employee in the Office of Financial Management.

Records Management 103 – Records Coordinators/Custodians – frequency = once

This course provides agency-appointed records coordinators with records management knowledge and information related to fulfilling coordinator responsibilities.

Contracting – Contract Managers – frequency = once

The goal of this course is to educate OFM Contract Managers about OFM-specific contracting processes and issues. This course is to be taken in addition to the DES-required contracts training.

A Path Towards Equity – all employees – frequency = once

This course focuses on foundational concepts to allow all employees to gain awareness of racial inequalities and how they show up in every system and workplace in Washington.

OFM Foundations in DEI– supervisors only – frequency = once

This is a required training for OFM supervisors, but open to all staff. The goal is to build knowledge and skills for growing more effective cross-cultural relationships and partnerships.

The OFM learning management tool tracks these employee trainings.

Privacy

OFM Privacy Program

Housed within OFM, ERDC follows OFM's privacy program, as well as a set of more specific privacy principles to follow. OFM's privacy program moves the idea of privacy into a culture of privacy by identifying our compliance obligations associated with data, combining those compliance obligations with best practices and then aligning OFM policy and internal controls to reflect a high level of data stewardship in the protection of confidential information. A privacy program gives us a framework for managing privacy-related issues consistently by creating policies and procedures at a functional level, hence, reducing risk and building trust.

OFM's privacy program is built with a broad base of support throughout OFM as each division nominated a privacy champion to work on development and implementation of the privacy program. The OFM Privacy Officer is responsible for the privacy program. The following privacy principles were adopted as OFM Policy #4.01 Privacy Program:

Security. We protect the confidential information entrusted to us against unauthorized access. Confidential Information is specific information that is not disclosable or is made confidential by law or for which special handling is required.

Data Minimization/Purpose Driven. We limit the collection, access, and use of confidential information to only what we require to provide OFM services and retain it only as long as necessary to meet our business need and legal requirements.

Transparency. We are transparent about what confidential information we collect, why we collect it, and how it is used.

Accountability. We are accountable for collecting, using, managing, and dispositioning confidential information in a manner that is consistent with best practices and as required by law, OFM policies and procedures.

Value Driven. We are respectful of privacy rights associated with confidential information entrusted to us.

Culture Driven. We will ensure that OFM staff have access to relevant privacy training, resources and guidance.

Due Diligence/Lawful Use. We only share confidential information consistent with the law and under an OFM agreement. Agreements shall include instructions about how confidential information is protected. For public records, we shall apply all applicable exemptions before sharing records containing confidential information. For all confidential information shared, we shall apply data minimization principles and redactions as possible.

ERDC Privacy Principles

ERDC values the protection of privacy for students, employees and employers and is guided by the following privacy priorities, which have been adopted from the OFM and enhanced to meet our specific organizational needs focused on education data and research:

Lawful, fair & responsible use. ERDC data collection, use, and disclosure is based on legal authority. The ERDC collects, uses, and disclosed information responsibly and ethically, avoiding discrimination, deception, or harm. ERDC follows privacy laws, such as FERPA, to safeguard the confidentiality of data. ERDC's privacy practices are also guided by OCIO Policy 141.10 and the Washington State Agency Privacy Principles.

Data minimization. ERDC collects, uses, or discloses the minimum amount of information to accomplish the stated purpose for collecting the information. We categorize data in order to guide our procedures for accessing the data.

Purpose limitation. The aim of ERDC is to make education data available to policy-makers and state organizations that make decisions related to Washington students, while also protecting the data ERDC collects pursuant to state law. Several state laws articulate the reasons for collecting information through the ERDC P20W data warehouse. See RCW 43.41.100 for more on the creation of the Education and Research Data Center.

Transparency & accountability. The ERDC strives for both transparency and accountability. Transparency means being open and transparent about what personal information is collected, for what purposes, and who it is shared with under what circumstances. Accountability means being responsible and answerable for following data privacy laws and principles.

Due diligence. The ERDC takes reasonable steps and exercises care before and after entering into data use agreements with state agencies and third parties that include sharing personal information.

Security. ERDC uses appropriate administrative, technical and physical security practices to protect the confidentiality, integrity, availability and control of personal information. ERDC maintains a regularly updated Data Security Manual

P20W People Roles: Data Contributor Roles & Opportunities

Several organizations contribute data to the ERDC. Some of these contribute directly to the P20W, while others share data with a more specific and/or limited scope. ERDC signs a data sharing agreement with each agency listed above that outlines several components, including but not limited to the purpose of sharing data with ERDC, data access, security, and disposition, as well as language regarding redisclosures. Each agreement with the data contributing agency is negotiated independently.

Not all of the data that is provided to ERDC is available for request. For more details about what data is available to request from our data contributors, please consult the Washington State ERDC P20W Data Handbook.

Roles & Responsibilities of Data Contributing Agencies

The ERDC developed a Memorandum of Understanding with its data contributors in 2011, which was again updated in 2020. This is posted on our website.

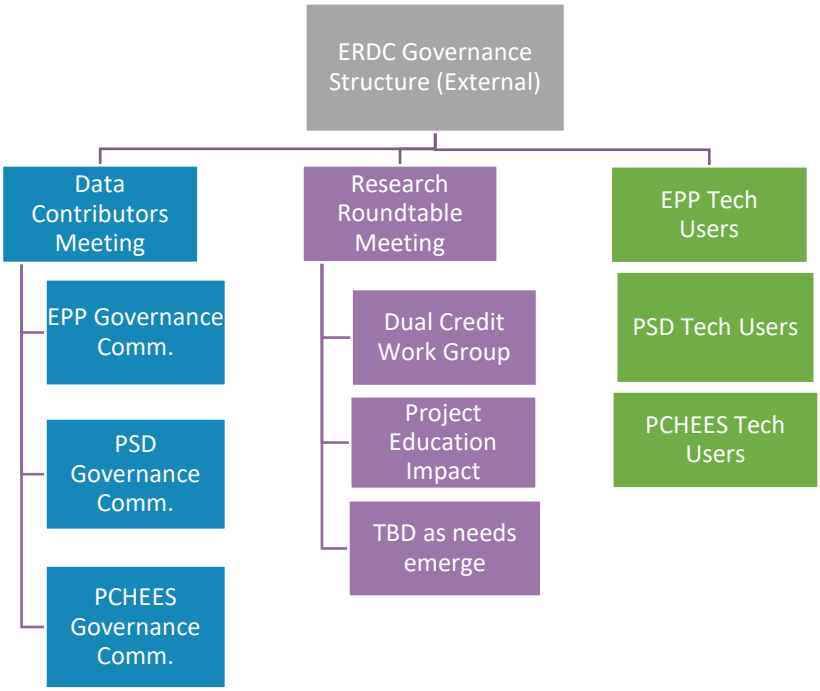
RCW 43.41.400 mandates that ERDC shall make data from collaborative analyses available to the education agencies and institutions that contribute data to the education data center to the extent allowed by federal and state security and confidentiality requirements applicable to the data of each contributing agency or institution. Part of our governance strategy is ensuring that we have a regular gathering with data contributors to keep them informed and discuss pressing issues. In addition, ERDC asks that data contributing agencies:

- Act as subject matter experts for domain-specific data
- Ensure the stability of the technology solution by:
    - Communicating to ERDC with sufficient time, changes in data structure or format.
    - Communicating internal business technology changes which could affect the delivery of data to the ERDC system.
    - Providing reasonable assistance in resolving data loading issues which are attributed to the data agency.
- Review ERDC products and products created by data requestors
- Provide quality assured data
- Provide a data dictionary
- Attend P20W Quarterly Data Contributor's Group meetings on a regular basis

Partnership Opportunities

As ERDC's data systems and research evolves, it is important to maintain a system of feedback that incorporates the voices of data contributors, data users, and the public at large. Creating spaces for transparent communication, to solicit feedback, and to share how data is accessed and used is key to a healthy P20W data system. ERDC has a governance structure that allows for distinct conversations about data governance, research, and technical needs. Further, this structure allows for cross-functional sharing so that rather than operating in silos, committees learn from each other to inform and guide their conversations. The purpose and membership of each meeting/committee is described in more detail below.

These committees are subject to change as needs shift over time, but in general will follow this structure.



Governance Focused Groups

P20W Data Contributors Meeting

The ERDC hosts a quarterly gathering for all state agency and higher education partners that share data with ERDC for use in the P20W data system. There are three primary purposes of this group:

1) To create a space for agencies to collaborate on research priorities
2) To create a space for agencies to share legislative priorities and updates
3) To keep ERDC data contributors informed about ERDC updates related to research and data governance; as well as keep ERDC informed about topics important to data contributors.

Governance Committees

The purpose of these committees is to discuss and evaluate the utility of proposed changes to existing data collections, new data collections, and timing of data collections. against the emerging legislative and research needs specific to the ERDC data collections. When needed, these spaces can also be reserved for discussing data sharing agreements pertinent to the collections. Membership is limited to representatives of the institutions that contribute data or their designees. There is currently a governance committee for each data collection administered by ERDC:

- Educator Preparation Program (EPP) Governance Committee
- Postsecondary Student Data Collection Governance Committee
- Public Centralized Higher Education Enrollment System (PCHEES) Governance Committee

Research Focused Groups

Research Roundtable

The purpose of this group is to share knowledge about current trends and emerging needs in education research. Guided by the ERDC Critical Questions and Research Agenda, this is a space for ERDC to share research findings, seek input from experts in the field, and to share new ideas. Guest presenters and collaborative projects are also encouraged. This group will annually review "additional data needs" to help inform new ideas for ERDC managed data collections or requests from ERDC's data contributing agencies.

Research Advisory Committees

The purpose of these committees is to provide specific support on ERDC research projects. Because research projects change, the focus of these groups may also shift over time. Membership varies by group. If you are interested in learning more, please email erdc@ofm.wa.gov. As of February 2024, the research advisory committees include:

- Dual Credit Work Group (ERDC hosts)
- Project Education Impact (ERDC participates)
- Early Learning Group (ERDC hosts)
- Additional groups to be created as determined by legislative priorities and the ERDC Research Agenda

Data Collection Technical Committees

The purpose of these groups is ensuring data quality and timely submission through ongoing review of the technical aspects of the collection infrastructure. Topics of discussion include work performed by ERDC staff to maintain, expand, and improve upon the functionality of the system, and challenges encountered by institution staff in submitting accurate information. Data elements required for submission are also reviewed to ensure the methods for accurately representing how students enroll in and complete their educational journey are adequate. Membership is limited to representatives of the institutions that contribute data, typically data analysts from institutional research or registrar's offices.

- Educator Preparation Program (EPP) Technical Users Committee

- Postsecondary Student Data Collection Technical Users Committee
- PCHEES Technical Users Committee

If you are interested in participating in any of the partnership opportunities named in this document or you have questions about ERDC or our governance program, please contact erdc@ofm.wa.gov.