1601POL Protection of Personally Identifiable Information (PII) (Rev3)

Effective Date: November 2020
Last Modified: March 2026

To provide services to job seekers and other WorkSource System customers, Olympic Workforce Development Council (OWDC) staff, subrecipients, contractors and partners collect and store a variety of protected, personal identifiable information (PII). OWDC is committed to ensuring appropriate use, storage, and protection of PII from unauthorized use or disclosure that aligns with federal Workforce Innovation and Opportunity Act (WIOA) law, regulation, guidance, and applicable Washington state policy (1026(rev1)).

1. **Confidential PII Records** include entire record systems, specific records or individual identifiable data.
   a. Records may include but are not limited to documents, file content, computer files, letters, and other notations of records or data.
   b. PII may include, but is not limited to, Social Security numbers, driver's license numbers, financial account information, medical information, dates of birth, home addresses, personal email addresses, or other information that can be used to distinguish or trace an individual identity.
2. **Subrecipients are required to employ proactive methods for protecting PII, including internal controls and written policies and procedures for safeguarding PII in compliance with 2 CRF 200.303. Including methods for collecting, maintaining, storing, purging, and securely transmitting PII.**
   a. Subrecipients, contractors, and partners must ensure that access to PII is limited to authorized personnel who require the information to perform official duties.
   b. Subrecipients must ensure that all employees handling PII receive appropriate training on safeguarding confidential information and comply with all applicable federal, state, and local confidentiality requirements.
3. **Protection of PII: Physical documents that contain PII,** such as (participants' or family members') social security numbers, driver's license, birth certificates, or I-9 documents, must be stored in a confidential, locked file cabinet, only accessible by appropriate staff.
   a. At no time should any staff retain PII on personal devices or unsecured networks.
   b. **Computers that have access to PII data** must be locked when not in use and anytime a staff person is not attending their workstation.
   c. **All staff with access to online systems containing PII** must follow the procedures established by the administering agency. Electronic information and data are subject to all the requirements of this policy.
   d. PII transmitted electronically must be sent using secure or encrypted methods approved by the administering agency. PII must not be transmitted through unsecured email, public file sharing platforms, or other unapproved methods.
   e. Printed documents containing PII must not be left unattended in public or shared workspaces and must be secured when not actively in use.
4. **Staff and subrecipients are required to ensure the privacy of all PII and to protect such information from unauthorized disclosure.** Loss of PII can result in substantial harm to individuals, including identity theft or other fraudulent use of this information.

- Maintain PII in accordance with the standards for information security described in *TEGL 39-11.*
- Ensure that during the performance of each grant/contract, PII has been obtained in conformity with applicable Federal and State laws governing the confidentiality of information.
- If improper use of PII or unauthorized access to PII occur, staff are required to immediately notify OWDC Program Supervisor and Program Analyst of the breach.
    - Notification must occur as soon as possible upon discovery of the incident so that appropriate steps can be taken to mitigate potential harm.
    - OWDC staff will coordinate notification to appropriate state agencies, partner organizations, and affected parties as required and will implement correction action procedures to prevent future occurrences.

5. **Data Retention and Destruction: PII must be retained only for the period required under applicable federal and state record retention requirements.**
    a. When PII is no longer required, records must be destroyed using secure methods that prevent reconstruction of the information. Acceptable methods include shredding paper records and permanently deleting or securely wiping electronic files.
6. **Failure to comply with the *TEGL 39-11* requirements may result in disciplinary action.**
    - Subrecipient's improper use of PII for an unauthorized purpose may result in the termination or suspension of the contract, the imposition of special conditions or restrictions, or other actions the OWDC deems necessary to protect the privacy of participants or the integrity of data.

References

Guidance on the Handling and Protection of Personally Identifiable Information, Training and Employment Guidance Letter, TEGL 39-11

Personally Identifiable Information, Subpart A – Acronyms and Definitions, Code of Federal Regulations Title 2, Subtitle A, Chapter 11 Part 200, 2 CFR §200.79 & 2 CRF § 200.303.

Records Retention and Public Access, Workforce Innovation and Opportunity Act Policy 5403 (Rev1)

Safeguarding Personally Identifiable Information (PII), WorkSource System Policy 1026 (Rev1)