

Privacy, Security, and Protecting Personally Identifiable and Sensitive Information

Purpose:

This policy establishes requirements to ensure privacy, security, and confidentiality of Personally Identifiable Information (PII) and sensitive data collected, maintained, and shared through programs funded through the local workforce development area.

This policy ensures compliance with:

- [Privacy Act of 1974](#)
- [Freedom of Information Act](#) (FOIA)
- Federal and state regulations
- US DOL Guidance

Audience:

This policy pertains to the following individuals:

- NWPA Job Connect (Workforce Development Board) members and staff
- Program service providers and their staff
- Grantees and sub-grantees
- PA CareerLink® employees
- Any agency providing services funded through NWPA Workforce Development Area.

Definitions:

Personally Identifiable Information (PII): Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifiable information.

Protected PII: Information that if disclosed could result in harm to the individual linked to the information. Examples include social security numbers, credit card numbers, bank account numbers, home telephone numbers, ages, birthdates, marital status, spouse names, educational history, biometric identifiers, medical history, financial information, and computer passwords.

Non-sensitive PII: Information that if disclosed, by itself, could not reasonably be expected to result in personal harm. This is stand-alone information that is not linked or closely associated with any protected or unprotected PII. Examples include first and last names, e-mail addresses, business addresses, business telephone numbers, general educational credentials, gender or race. However, a combination of these items could potentially be classified as protected or sensitive PII.

Policy:

The following steps must be followed when working with individuals who are applying for and receiving funds.

A. Security Requirements:

- Staff must keep all PII confidential
- Use unique identifiers when possible
 - If SSN must be used, truncate (e.g., last 4 digits)
- Files must only contain participant's information
 - Remove/redact unrelated names (e.g., rosters)
- Ensure accurate and timely data into CWDS, state system of record
- When transporting PII and sensitive data:
 - Use locked containers
 - Maintain a document control log
 - Do not leave information unattended

B. Technology and Data Security Controls:

- Encryption is required for sensitive data
 - PII must be encrypted or redacted for transmission
- Only authorized devices may access PII
 - Personal devices may not store PII
- Use secure connections
- Avoid public Wi-Fi unless protected
- Devices must be:
 - Password protected
 - Have encryption enabled
- Lock devices when unattended
- Access only necessary information
- Do not share passwords
- Report missing equipment to the manager. Include item missing, equipment ID #, and the situation.

C. Participant Information:

- Collect only required information
- Protect privacy during conversations
- Obtain written consent before collecting or sharing data
- Maintain a signed Release of Information Form
 - Release of Information must contain:
 - Purpose of data use
 - Who may receive the data
 - End date of consent
 - How consent can be revoked
- Medical Information:
 - Staff must keep medical documents in a separate file

- Medical files must be stored in a locked and secure location. These must be separate from other program participant files.
- Information must only be shared with authorized individuals.

D. Authorized Disclosure of Information:

- PII may only be shared when:
 - Written consent is provided by the individual
 - Required for an audit
 - Required by law

E. Breach Reporting and Response:

In the event, a breach occurs (unauthorized access, disclosure, or loss of PII), the following steps must occur:

- Report within 24 hours to:
 - Supervisor
 - IT/Security
 - NWPA Job Connect Director
- Report must include:
 - Description of incident
 - Type of data involved
 - Number of individuals affected
 - Actions taken
- Response:
 - Contain and secure data
 - Investigate impact
 - Implement corrective actions

F. Disposal of Personal Information:

Disposal of personal information will follow federal and state requirements and the [NWPA Job Connect Record Retention Policy # 303](#).

- Shred sensitive information.
- Securely delete sensitive electronic PII, including degaussing magnetic tape files.

G. Training:

- Mandatory PII training upon hire
- Annual refresher training
- Additional training when the policy or risks change
- All staff must sign the Privacy, Security, and Protecting Personally Identifiable and Sensitive Information Form annually.
 - Signed forms must be submitted to NWPA Job Connect Monitor.

REFERENCE

2 CFR 200.303

20 CFR 680.110

Privacy Act of 1974

Freedom of Information Act (FOIA)

USDOL Training and Employment Guidance Letter (TEGL) No. 39-11

HISTORY

Name	Date	Rev. Level	Description of change	Effective Date
Susan Richmond	2/25/2026	A	New Policy- Combined Confidentiality, Privacy, and PII	

Recissions:

NWPA Job Connect #306 Personally Identifiable Information Policy

NWPA Job Connect #307 Confidentiality Policy

NWPA Job Connect #308 Privacy Policy

Privacy, Security, and Protecting Personally Identifiable and Sensitive Information Sign Off Form

I have reviewed and acknowledge the NWP Job Connect's Privacy, Security, and Protecting Personally Identifiable and Sensitive Information Policy. I agree that all necessary steps will be taken to ensure the privacy and confidential nature of all personally identifiable information (PII) to protect such information from unauthorized disclosure.

I further agree that all PII will be stored in an area that cannot be accessed by unauthorized persons. Storing of information will be managed with appropriate information technology (IT) services and in designated locations. Access to any PII through program and grant activity will be restricted to only those individuals who need access in their official capacity to perform duties in connection with the scope of work.

Printed Name

Signature

Agency Name

Date