



USE AND CONFIDENTIALITY OF PARTICIPANT PERSONALLY IDENTIFIABLE INFORMATION (PII)

INTRODUCTION

It is the policy of the Workforce Development Board of Solano County (WDB) to protect the privacy of all applicants for program services, as well as the privacy of all customers and clients receiving program services. The purpose of this policy is to describe how the WDB will protect all personally identifiable information (PII) on applicants and customers, and the consequences for not adhering to these safeguards.

Under the Workforce Innovation and Opportunity Act (WIOA) and other programs administered by the WDB, staff obtains personal and confidential information from individuals for purposes including eligibility determination, enrollment, service delivery, case management, performance reporting, monitoring, evaluation, and other authorized program administration. The WDB must take reasonable measures to safeguard protected personally identifiable information and other information designated as sensitive, consistent with applicable Federal, state, and local laws regarding privacy and obligations of confidentiality.

Personal information will be treated in the strictest confidence and will not be disclosed outside of the WDB without appropriate written authorization, except when disclosure is required or authorized by law, regulation, grant requirements, data sharing agreements, monitoring or auditing requirements, or other authorized program administration purposes.

QUESTIONS

Questions relating to this policy should be directed to Tracy White, Director of One-Stop Operations, at twhite@solanowdb.org or at 707-863-3520.

ATTACHMENTS

- Attachment A: Staff/Representative Confidentiality Agreement
- Attachment B: Participant Confidentiality Rights
- Attachment C: Definition of Key Terms

RESCISSIONS

This policy replaces and supersedes WDB 2018-01 – Use and Confidentiality of Participant Personally Identifiable Information (PII) and WDB 2018-01, Change 1 – Use and Confidentiality of Participant Personally Identifiable Information (PII), Change 1.

POLICY

Employees, contractors, consultants, and volunteers of the WDB (herein "staff and representatives") may be exposed to participant information which is confidential and/or privileged and proprietary in nature. As part of grant activities, staff and representatives may have access to large quantities of personally identifiable information (PII) relating to the WDB, its employees, subrecipients, contractors, partner organizations, employers, applicants, and program participants. This information is generally found in

personnel files, participant data sets, performance reports, program evaluations, grant and contract files, and other sources.

The WDB expects all staff and representatives to respect the privacy of clients and to maintain their personal and financial information as confidential. Access to any PII and other sensitive information must be restricted to only those staff and representatives who require access in their official capacity, and access must be limited to the minimum information necessary to perform their authorized duties under the applicable grant, contract, subaward, agreement or program.

Staff and representatives must not access, extract, use, copy, remove, transmit, or disclose participant data or other sensitive information for any purpose that is not authorized by applicable law, regulation, grant, contract, subaward, data-sharing agreement or approved WDB program procedure. PII and other confidential information may be disclosed only to individuals or entities authorized to receive it and only for an authorized program or business purpose. No information may be released without appropriate authorization.

CUSTOMER AWARENESS

Individuals must be informed in writing about the types information collected, the purpose for which the information will be used, the circumstances under which it may be disclosed, whether providing the information is voluntary or required, any consequences of declining to provide required information, and the safeguards used to protect their information.

The written notice must explain that personal and confidential information:

- May be shared among federal, state, and local agencies, partner organizations, contractors, subrecipients, auditors, monitors, and service providers when necessary for an authorized program purpose;
- Will be used only for authorized purposes, including eligibility determination, enrollment, service delivery, case management, referrals, performance reporting, monitoring, auditing, evaluation, data validation, wage-record matching, and other legally authorized program administration activities; and
- Will be protected through administrative, physical, and technical safeguards.

When participant information will be shared for a purpose that is not otherwise required or authorized by law, regulation, grant requirements, monitoring or auditing requirements, or an applicable data-sharing agreement, the individual must read, sign, and date an appropriate Release of Information before the disclosure occurs.

Individuals must be informed that they may decline optional disclosures or referrals to partner agencies when written authorization is required. Declining an optional disclosure will not, by itself, affect eligibility for services; however, staff must explain when certain information is required to determine eligibility, provide a requested service, comply with program reporting requirements, or satisfy another legal or grant requirement. Staff and representatives must take reasonable administrative, physical, and technical measures to reduce the risk of unauthorized access, use, or disclosure of sensitive information and PII, including:

- Collecting and retaining only the minimum information necessary for the authorized purpose;
- Limiting access to individuals with an authorized business need; and
- Using encryption, strong authentication procedures, access controls, and other appropriate safeguards to make information inaccessible or unusable by unauthorized individuals.

PROTECTING INFORMATION

PII and other sensitive or confidential information require appropriate safeguards to protect against unauthorized access, use, disclosure, modification, loss, or destruction. Confidentiality means that

information, records, reports, and other data are accessible, used, and disclosed only by authorized individuals and only for authorized purposes.

Staff and representatives must follow all administrative, physical, and technical safeguards established by the WDB when collecting, accessing, using, storing, transmitting, transporting, or destroying confidential information to protect the privacy of applicants and participants.

Physical Data Protection Requirements

All PII and other sensitive or confidential information must be stored in an area that is physically protected from access by unauthorized persons. Staff and representatives must not leave personal or confidential information open, visible, or unattended.

When a staff or representative's workstation is unattended, all documents containing PII or other confidential information must be secured in a locked drawer, cabinet, office, or other approved storage location. Work surfaces, printers, fax machines, photocopiers, and other shared areas must be kept clear of confidential documents when the documents are not actively being used. At the end of the workday, all such documents must be secured. Computer screens must be locked whenever the user leaves the workstation unattended.

Paper records containing PII or other confidential information must remain at an authorized WDB worksite unless removal is necessary for an authorized business purpose. Staff must obtain prior approval from their supervisor or Division Director before removing such records from the workplace, except when transportation is already required as part of an established WDB or County procedure, such as the direct delivery of invoices to the County Accounting Offices.

When transporting hard-copy PII or other confidential information, the records must remain under the control of the authorized employee or be secured in a locked container when not in use. Only the minimum records necessary for the authorized purpose may be transported, and the records must be returned to an approved secure location as soon as practicable. Unattended paper files or electronic devices containing PII must be stored in a non-visible area of a locked vehicle, such as the trunk, and may not be left in a vehicle overnight or for another extended period. A vehicle is not an approved long-term storage location.

All discarded paper containing confidential information must be placed in a locked shredder bin or destroyed using another approved secure method.

Participant files retained for program administration, performance, monitoring, or archival purposes must be appropriately identified and stored in a manner that alerts authorized staff to their confidential nature without unnecessarily exposing or displaying sensitive information.

Participant PII and other confidential records must be retained only for the period required by applicable federal, state, and local law, grant or contract requirements, records-retention schedules, monitoring or audit requirements, or any applicable litigation hold or investigation. At the end of the applicable retention period, and when no audit, monitoring review, investigation, claim, or litigation hold is pending, the records must be securely destroyed using an approved method that renders the information unreadable and incapable of reconstruction. When an outside destruction vendor is used, the vendor must be appropriately qualified and authorized, and documentation of destruction must be maintained as required.

Electronic Data Protection Requirements

To safeguard WDB's electronically stored data, each user will receive a designated and authorized log-on and password that restricts the user to the applications or functions commensurate with their assigned

responsibilities, supporting an appropriate segregation of duties. Log-on credentials and passwords must not be shared. Access must be modified or removed when the user's responsibilities change or when the user no longer has an authorized business need for access. These controls help ensure that unauthorized persons cannot reasonably retrieve the information by means of a computer or other electronic device.

The WDB requires all staff and representatives to secure mobile equipment, such as laptop computers and other devices that may have PII stored on them. Devices must be password protected and safeguarded when not in use. Any device that is lost, stolen, misplaced, or believed to be compromised must be reported immediately in accordance with the Security Breaches section of this policy.

Accessing or storing data containing PII on personally owned equipment is strictly prohibited, regardless of location. PII may not be accessed, stored, or transmitted using non-WDB-managed IT services, including personal or third-party email accounts and unauthorized cloud-based storage services.

TRANSMISSION OF CONFIDENTIAL INFORMATION

Staff and representatives must avoid communicating sensitive information or PII about an applicant or participant to partner agencies or other staff via email whenever possible. If transmission by email is necessary, staff and representatives must verify that the intended recipient is authorized to receive the information, limit the information to the minimum necessary for the authorized purpose, and ensure that the recipient understands their responsibility to protect the information. Staff and representatives must only communicate sensitive information or PII through WDB-authorized email accounts and not through third party or personal email accounts.

PII and other sensitive data transmitted via email or stored on mobile data storage, such as thumb drives or external hard drives, must be encrypted. Staff and representatives must not transmit unencrypted sensitive PII to any entity, including the Department of Labor, WDB staff, or contractors. Staff and representatives should discourage participants from emailing personal and confidential information to their case managers and should provide an approved secure method for submitting such information whenever available.

When conducting virtual meetings or video conferencing, staff and representatives must take reasonable precautions to ensure that PII is not visible or audible to unauthorized individuals. Screen sharing of documents containing PII should be limited to only what is necessary and only with authorized participants.

Any information posted to social media sites may be considered public record and is subject to public disclosure. No sensitive information or PII may be posted to social media sites under any circumstances.

Staff and representatives must take reasonable precautions to ensure that unauthorized individuals do not overhear any discussion of confidential information, whether in person or through electronic means.

SOCIAL SECURITY NUMBERS

Social security numbers are protected as high-risk information. When requesting a participant's social security number, staff and representatives should explain whether disclosure is voluntary or required, how the social security number will be used and how the participant's privacy will be protected.

Staff must request a participant's social security number when offering the following services:

- Staff-assisted service related to eligibility determination, enrollment, job search activity, employment, and performance reporting;
- Training and educational services;
- Wage-record matching, program evaluation, and other authorized reporting purposes; and
- Registering for or use of CalJOBS, consistent with current CalJOBS requirements.

However, an individual is not required to provide their social security number to receive WIOA services, and services cannot be denied to an individual declines to disclose their social security number. When an individual declines to provide a social security number, staff shall follow current CalJOBS requirements and established WDB procedures for assigning and using a pseudo social security number or other system generated identifier.

Whenever possible, staff and representatives should use unique identifiers for participant tracking instead of social security numbers. Although social security numbers may be needed for initial eligibility or authorized performance reporting, wage-record matching, or legally permitted program purposes, a unique identifier should be linked to each individual record and used thereafter whenever feasible. This includes training, contract, payment, and other program-related documents. If a social security number is to be used for an authorized purpose, it must be stored securely and disclosed or displayed only to the extent necessary for that purpose. For example, a training document should not include the participant's name and social security number, rather the participant's name and a truncated social security number.

Social Security numbers may not be displayed on documents mailed to a participant or to another entity unless required by law for an authorized form, application, or program purpose. A social security number may not be printed on the outside of an envelope or be visible through an envelope window. Social Security numbers shall not be included in email subject lines, left in voicemail messages, sent by text message, or transmitted through any other unsecured electronic messaging platform.

MEDICAL AND DISABILITY RECORDS

Medical and disability records are additionally protected as confidential information. To ensure the information is protected, any medical or disability record must be kept separately from working participant files and kept in a secure physical and/or electronic location. Only the portion of the participant's information that reveals the presence of a disability or other data element should be included in the participant's file to minimize staff and representative access to medical files.

Once collected, access to the medical file should be limited and only accessed:

- With the approval of program management and only when necessary for WIOA service delivery;
- By first aid and safety personnel in the event of an emergency; or
- By local, state, or federal monitors.

Electronic medical and disability records must be stored in a secure location separate from the participant's general electronic file, with access limited to authorized personnel only. Staff and representatives should not store medical or disability information in CalJOBS beyond what is necessary to document a participant's eligibility or service needs.

When all WIOA or other WDB services are complete and the participant file is ready to be archived, participant medical and disability-related information must be placed in a sealed envelope and marked "Medical and Disability Information" for physical files. For electronic files, medical and disability-related information should be secured in a restricted access location and clearly identified as containing sensitive medical information.

SECURITY BREACHES

Any staff or representative who becomes aware of any actual or suspected PII security breach involving the inadvertent or intentional release of, loss of, or unauthorized access to confidential information, including PII, shall immediately inform their direct supervisor. PII security incidents include, but are not limited to, any event (intentional or unintentional) that causes the loss, damage, or destruction, or unauthorized access, use, modification, or disclosure of information assets. The system or device affected by a PII security incident shall be immediately removed from operation shall remain removed from operation until correction and mitigation measures are applied.

Supervisors should assess the likely risk of harm caused by the breach and then assess the level of breach. Supervisors should bear in mind that notification when there is little or no risk of harm might create unnecessary concern and confusion.

The following four factors should be considered to assess the likely risk of harm:

- Nature of the Data Elements Breached
- Number of Individuals Affected
- Likelihood the Information is Accessible and Usable
- Likelihood the Breach May Lead to Harm

The WDB will inform the California Employment Development Department of security breaches when required by applicable state or federal law, grant requirements, data-sharing agreements, or other applicable notification requirements. Breaches subject to notification requirements include both electronic systems as well as paper documents.

Where a breach is determined to pose a risk of harm to affected individuals, the WDB will take reasonable steps to notify those individuals in a timely manner, consistent with the needs of law enforcement and any measures necessary to determine the scope of the breach and restore the integrity of the system.

All security breaches, regardless of severity, should be documented. Documentation should include a description of the breach, the data elements involved, the number of individuals affected, the actions taken to address the breach, and any corrective measures implemented to prevent future occurrences. The WDB will take prompt and appropriate corrective action when any evidence of a breach or violation is found.

COMPLIANCE

All staff and representatives with access to participant PII and/or confidential information must sign an acknowledgement before being granted access to PII, confirming that they have read the policy, understand the confidential nature of participant data and the potential sanctions for improper disclosure, and agree to abide by all other requirements and terms contained therein. This acknowledgement must be signed annually and upon any significant update to this policy.

Staff and representatives should participate in PII and data security training on at least an annual basis to ensure awareness of current requirements, best practices, and any updates to applicable federal, state, or local guidance. Documentation of completed training should be maintained by the WDB.

The WDB will ensure that any subrecipients or contractors who have access to PII obtained through ETA grant activities are informed of and required to comply with their responsibilities to protect such information. PII data obtained through ETA grant activities must not be disclosed to anyone other than those authorized under the applicable grant agreement.

Unauthorized disclosure of confidential or privileged information is a serious violation of this policy. Any failure to comply with confidentiality requirements identified in this policy may result in termination or suspension of contract or employment, or the imposition of special conditions or restrictions to protect the privacy of participants or the integrity of PII data. Misuse or noncompliance with PII data safeguards could lead to civil and criminal sanctions per federal and state laws.

Staff and representatives are expected to return materials containing privileged or confidential information at the time of separation from employment or expiration of service.

ETA DATA REQUIREMENTS

The WDB recognizes its specific obligations with respect to data obtained through Employment and Training Administration (ETA) grant activities. The following requirements apply to all ETA-related data and PII.

The WDB must not extract information from data supplied by ETA for any purpose not stated in the applicable grant agreement. All ETA-supplied data must be used solely for the purposes outlined in the grant agreement and in accordance with applicable federal regulations and guidance.

The WDB must permit ETA and its designated representatives to make onsite inspections during regular business hours for the purpose of conducting audits and other investigations to ensure compliance with confidentiality and data protection requirements. The WDB must make all records applicable to the grant agreement available to authorized persons for the purpose of inspection, review, and audit in a timely and cooperative manner.

PII and other data received from ETA must be retained only for the period of time required to use it for assessment, performance, or other grant purposes, or to satisfy applicable Federal records retention requirements. Upon expiration of the required retention period, and when no audit, investigation, claim, or litigation hold is pending, all such data must be destroyed in a secure manner, including the deletion of electronic data files and the physical destruction of any paper records containing ETA-supplied PII. Documentation of data destruction should be maintained by the WDB.

The WDB will ensure that these requirements are communicated to and observed by any subrecipients or contractors who have access to ETA grant data.

DISCLAIMER

This policy is based on WDB's interpretation of the statute, along with the Workforce Innovation and Opportunity Act; Final Rule released by the U.S. Department of Labor, and federal and state policies relating to WIOA implementation. This policy will be reviewed and updated based on any additional federal or state guidance.

REFERENCES

Law

- Workforce Innovation and Opportunity Act of 2014 (WIOA)
- Privacy Act of 1974, Section 7
- California SB168, Title 1.81.1 – Confidentiality of Social Security Numbers
- California AB763 – Privacy: Social Security Numbers
- California Civil Code §§1798.85–1798.89, Title 1.81.1 – Confidentiality of Social Security Numbers
- California Civil Code §1798.29 – Security Breach Notification Requirements for California Public Agencies
- 29 CFR §38.41 – Collection and Maintenance of Equal Opportunity Data and Other Information
- Federal Information Security Management Act of 2014(FISMA)

Federal Guidance

- 2 CFR 200.303(e) – Uniform Guidance: Internal Controls and Safeguarding of PII
- Training and Employment Guidance Letter (TEGL) 05-08 – Policy for Collection and Use of Workforce System Participants' Social Security Numbers
- TEGL 39-11 – Guidance on the Handling and Protection of Personally Identifiable Information (PII)
- OMB Memorandum M-07-16 – Safeguarding Against and Responding to the Breach of Personally Identifiable Information

- NIST SP 800-122 – Guide to Protecting the Confidentiality of PII
- NIST SP 800-63B – Digital Identity Guidelines: Authentication and Lifecycle Management

State Guidance

- State of California Department of Social Services All County Letter (ACL) 19-56 – 2019 CDSS Privacy and Security Agreement (PSA)
- • Workforce Services Directive WSD20-11 – Pseudo Social Security Number in CalJOBS
- • Workforce Services Directive WSD24-12 – CalJOBS System Access
- • Workforce Services Directive WSD24-13 – Local Area MIS Administrator and WSB CalJOBS SPOC Roles and Responsibilities

Approved by

Workforce Development Board of Solano County



WORKFORCE DEVELOPMENT BOARD

OF SOLANO COUNTY

STAFF/REPRESENTATIVE CONFIDENTIALITY AGREEMENT

I, _____ [print name] certify that I have read and understand the Workforce Development Board of Solano County's (WDB) policy on **USE AND CONFIDENTIALITY OF PARTICIPANT PERSONALLY IDENTIFIABLE INFORMATION (PII)**. I understand that I may have access to applicant, participant, customer, employer and other confidential records as part of my employment, contracting, consulting or volunteer work with the WDB. Confidential information provided to our agency by any participant or by any federal, state, or county entity is protected by law, regulation, and policy.

I understand that it is my responsibility as part of the workforce development system in Solano County to protect the confidentiality of all Workforce Innovation and Opportunity Act (WIOA) applicants and participants, as well as customers utilizing the Solano Employment Connection, an affiliate of the America's Job Centers of California (AJCC) system. I understand that in the workforce system's collection, usage, storage and transmission of customer information, the tenets of confidentiality are to be strictly enforced.

I understand that I have the responsibility to know whether information is protected. If I have any questions regarding whether particular information is confidential, I understand it is my responsibility to check with my supervisor.

I understand that unauthorized access, use, modification, or disclosure of confidential information is a crime under state and federal laws, including but not limited to California Information Privacy Act §1798.53-§1798.57, CA Penal Code §502, §2111 of the Unemployment Insurance Code, and §10850 of the Welfare and Institutions Code. I understand that violation of this policy could result in:

- Disciplinary action
- Termination of employment
- Criminal action (including incarceration)
- Civil action

By signing below, I agree to follow and be bound by the terms and conditions regarding confidentiality of personal information contained therein. WDB staff or their designee have answered any questions I may have had regarding this policy. I understand that this agreement must be signed prior to accessing any PII and must be renewed annually and upon any significant update to the WDB's Use and Confidentiality of Participant Personally Identifiable Information (PII) policy.

Signature: _____

Name: _____

Date: _____



WORKFORCE DEVELOPMENT BOARD

OF SOLANO COUNTY

PARTICIPANT CONFIDENTIALITY RIGHTS

Your privacy is one of our primary concerns. The Workforce Development Board of Solano County (WDB) makes every effort to provide you with a safe and private environment. The information below explains what information we gather, how we use it, when it may be shared, and how it is protected. It applies to WDB's use of information and is intended to protect the confidentiality of customer information.

Access to Data

Program staff collect data to document eligibility, provide services, manage programs, and comply with federal and state requirements under the Workforce Innovation and Opportunity Act (WIOA) and other WDB-administered programs. The WDB and its subcontractors will make every effort to collect and store data in a secure manner. Access to your personal and confidential information is restricted to staff and representatives who require the information in their official capacity, and access is limited to the minimum information necessary to perform their authorized duties.

Your personal and confidential information may be shared with authorized federal, state, and local agencies, partner organizations, contractors, auditors, monitors, and service providers when necessary for authorized program administration, monitoring, auditing, evaluation, performance reporting, data validation, wage-record matching, or other purposes authorized by law.

Use and Release of Data

We may ask you to provide personal information when you:

- Use the CalJOBS website;
- Request services, support, or information to validate eligibility;
- Share WDB content through social media;
- Subscribe to newsletters or other materials; or
- Contact us for information on services available.

Information we may request includes your email address, name, address, telephone number, proof of U.S. residence, proof of age, selective service verification, and other data elements depending on program eligibility criteria. Information collected will be used only for authorized purposes, including eligibility determination, enrollment, service delivery, case management, referrals, performance reporting, monitoring, auditing, evaluation, data validation, wage-record matching, and other authorized program administration activities. Upon request, data can be released to the subject of the information.

You may decide whether or not to provide your social security number unless disclosure is specifically required by law for a particular program or benefit. If you do not wish to provide this number, you can still receive WIOA services. Your social security number may be requested for authorized purposes, including eligibility determination, enrollment, employment-related services, performance reporting, wage-record matching, program evaluation, and CalJOBS registration or use. If you choose not to provide your social security number, staff will follow current CalJOBS requirements and WDB procedures for assigning and using a pseudo social security number or other system-generated identifier.

You may decline optional disclosures or referrals that require your written authorization. Choosing not to authorize an optional disclosure will not, by itself, affect your eligibility for services. However, certain

information may be required to determine eligibility, provide requested services, comply with program reporting requirements, or satisfy another legal or grant requirement.

How We Protect Your Data

To protect your personal information from unauthorized access and use, we use administrative, physical, and technical safeguards. These safeguards include computer protections, secured files, secured buildings, access limitations, encryption when required, and other measures designed to reduce the risk of unauthorized access, use, or disclosure.

All sensitive individual data is stored in an area that is physically safe from access by unauthorized persons. Data transmitted electronically is protected using approved safeguards. Medical and disability records are additionally protected as confidential information and are kept separately in a secured physical and/or electronic location. Social security numbers are protected as high-risk information. Whenever possible, staff and representatives use unique identifiers to track individual data rather than social security numbers or other personally identifiable information.

When conducting virtual meetings or video conferencing, staff take reasonable precautions to ensure that your personal information is not visible or audible to unauthorized individuals.

Disclosing Personal Information

The WDB may share your personal information with the California Employment Development Department, the U.S. Department of Labor, and other authorized monitors, auditors, agencies, contractors, partners, or service providers when necessary for authorized program purposes, programmatic or fiscal compliance, reporting, monitoring, auditing, evaluation, data validation, wage-record matching, or when otherwise required or authorized by law.

Any disclosure of your personal information that is not otherwise required or authorized by law, regulation, grant requirements, monitoring or auditing requirements, or an applicable data-sharing agreement will require your written authorization or, when applicable, the written authorization of your parent or legal guardian.

Notification of Privacy Changes

The WDB privacy rights are outlined in the Use and Confidentiality of Participant Personally Identifiable Information (PII) policy, which can be found on the WDB's website at: <https://solanoemployment.org/policies/>. The WDB reserves the right to make changes to this policy at any time. When changes are made, they will be posted and available with a revised effective date. We encourage you to periodically review the privacy policy.

Acknowledgement of Receipt

By signing below, I acknowledge that I have explained this agreement to the WDB-affiliated customer and provided the customer an opportunity to ask questions.

Staff Printed Name: _____

Staff Signature: _____ Date _____

By signing below, I acknowledge that I have read and understand this agreement. WDB staff have explained this agreement and answered any questions I may have had.

Individual Printed Name: _____

Individual Signature: _____ Date _____

(Parent / Guardian Name and Signature if under 18 years of age)

Definitions of Key Terms

Personally Identifiable Information (PII) as defined by OMB Memorandum M-07-16 is any information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal information that is linked or linkable to a specific individual.

There are two types of PII as defined by the U.S. Department of Labor in TEGL 39-11 that are based on the "risk of harm" that could result from the release of the PII:

- **Protected PII** – is any information that if disclosed could result in harm to the individual whose name or identity is linked to that information. Examples include, but are not limited to, social security numbers, credit card numbers, bank account numbers, personal telephone numbers, ages, birthdates, marital status, spouse names, educational history, biometric identifiers, medical history, financial information, and computer passwords.
- **Non-Sensitive PII** – is information that if disclosed, by itself, could not reasonably be expected to result in personal harm because it is not linked or closely associated with protected or otherwise sensitive information. Examples include first and last names, email addresses, business addresses, business telephone numbers, general education credentials, gender, or race.

A combination of non-sensitive PII could potentially be categorized as protected PII. For example, a name and business email address will not generally result in a high degree of harm to an individual. A name linked to a social security number and date of birth could result in identity theft.

Authorized Purpose means a use, access, disclosure, transmission, storage, or retention of PII or other confidential information that is permitted by applicable law, regulation, grant requirements, contract, subaward, data-sharing agreement, monitoring or auditing requirements, or approved WDB program procedure.

Minimum Necessary means limiting the collection, access, use, disclosure, transmission, or retention of PII or other confidential information to only the information reasonably needed to carry out the authorized purpose.

Pseudo Social Security Number means a system-generated unique identifier assigned in CalJOBS to a participant who declines to provide their social security number, used for tracking and case management purposes in lieu of an actual social security number.

Security Breach as defined by TEGL 39-11 is used to include the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users, or for a purpose other than an authorized purpose, have access or potential access to personally identifiable information, whether physical or electronic.

Sensitive Information as defined by TEGL 39-11 is any unclassified information whose loss, misuse, unauthorized access, or modification could adversely affect the conduct of Federal programs or the privacy to which individuals are entitled under the Privacy Act.

Staff and Representatives means WDB employees, contractors, consultants, and volunteers who may have access to participant PII or other confidential information as part of their work or service with the WDB.