Defining ‘trusted entities’ for the purposes of national data sharing

Appendix 5: Use case - Western Australian Government and the Department of Health, Disability and Aged Care

Use case information

Identifying Characteristic	Details
Use case name	PeopleWA
Date	09/2025
Data Requester	Various – government, researchers, not-for-profits, Aboriginal Community-Controlled Organisations
Data Custodian	Multiple
Data Characteristics	<20gb unit record de-identified data in a secure environment
Approved purpose	Research, policy development, service delivery/improvement, Closing the Gap
Approved timeframe	Various – a couple of months to ongoing requests
Legal basis for sharing	PeopleWA Memorandum of Understanding (MOU) *Privacy and Responsible Information Sharing Act 2024* (WA)
Additional Notes	This is general information on PeopleWA, rather than being related to a specific applicant seeking PeopleWA data. Requested data can only be accessed within PeopleWA’s secure access environment. The PeopleWA team undertake all relevant output vetting in line with the terms and conditions of PeopleWA and data custodians' requirements. As the asset is de-identified, the legal basis for sharing is not critical. If the data request meets the project requirements of access, then the data can be shared.

Alignment with attributes

The below table displays the alignment of the use case with the trusted entity attributes.

- **Strong alignment:** The data custodian required the data requester to provide significant evidence of the attribute to assess trustworthiness.
- **Partial alignment:** The data custodian required the data requester to provide some evidence of the attribute to assess trustworthiness.
- **Not assessed:** The data custodian did not assess the attribute, or it was not applicable.

Theme	Attribute	Strong alignment	Partial alignment	Not assessed	Reasoning for alignment with attributes
Transparency	**Verifiable audit and assurance processes** Where appropriate, internal and external processes will be implemented to verify compliance with legal and ethical standards, including those related to data environments and systems.			✓	Not applicable as data can only be accessed in PeopleWA's secure access environment.
Transparency	**Public transparency standards** The agency will have public-facing processes and/or standards for data release and publication.			✓	Not assessed as data custodians that provide data to the CVDL for linking are responsible for maintaining their own public transparency information.
Transparency	**Transparent and defined project methodology** Clear and transparent project methodologies, including integration approaches, output vetting and risk management procedures, will be documented and shared with the relevant data custodian.	✓			Data requesters are required to complete an application form that requests evidence of project methodologies. PeopleWA does complete some output vetting and risk management processes on behalf of the requester.
Accountability	**Legally supported sharing** Data sharing arrangements will be legally authorised and supported by clear documentation such as agreements and data sharing registers.	✓			PeopleWA want to understand how a requesting agency ensures staff understand and adhere to PeopleWA's terms, including MOUs and data use agreements.
Accountability	**Ethical consideration** Projects will undergo ethics consideration and where required approval, consent and review	✓			Data requesters need to advise ethics processes in place, including who they apply to, compliance and repercussions for non-compliance. Requesters should be

Theme	Attribute	Strong alignment	Partial alignment	Not assessed	Reasoning for alignment with attributes
	processes to ensure alignment with ethical standards.				able to demonstrate a track record of ethical data use, both at the individual and sector level, and should reflect a commitment to responsible data stewardship over time.
Accountability	**Defined roles and responsibilities** Agencies will have clear data roles and responsibilities to ensure accountability.	✓			Data requesters are required to have clearly defined roles for each project as covered by PeopleWA's terms and conditions.
Accountability	**Authorised and skilled personnel** Personnel will have the knowledge, skills, authorisation and training to use data appropriately, including training in data breach and risk management.	✓			
Data Management and Governance	**Data quality processes** Data quality management plans will be implemented to ensure data integrity and compliance.			✓	Not applicable as PeopleWA manage the quality of the asset and its outputs.
Data Management and Governance	**Data governance authorisations** Agencies will have established data governance processes which have clear decision-making authorisations. This includes an understanding of the agencies data governance priorities, dispute resolution processes and accountable data custodianship roles.		✓		PeopleWA are particularly focused on how the data is restricted to only staff approved to work on the project.
Data Management and Governance	**Defined metadata management practices with accountable data custodianship roles** Agencies will have defined metadata management practices which are accurate, consistent and accessible across the agency. This includes data lineage information.			✓	Not applicable as PeopleWA manage the metadata of the asset.

Theme	Attribute	Strong alignment	Partial alignment	Not assessed	Reasoning for alignment with attributes
Data Management and Governance	**Consistent and controlled data release protocols** Agencies will have clear operating models for data release, including for review, verification, and approval for release.			✓	Not applicable as PeopleWA manage data release procedures.
Data Management and Governance	**Established escalation and risk management frameworks** Agencies will have established escalation pathways for managing risks and incidents. Projects will have comprehensive risk management plans which consider privacy by design and security risk assessments.	✓			PeopleWA requires agencies to have risk management procedures.
Security	**Secure transfer mechanisms** Agencies have secure mechanisms for data transfer to prevent breaches.			✓	Not applicable as data is only accessible via PeopleWA's secure environment.
Security	**Secure access control mechanisms** Agencies will implement data safeguards, use secure access environments appropriate to the sensitivity of the data, and restrict data access to authorised users with appropriate security clearances.	✓			PeopleWA want to ensure that an agency's controls and safeguards align with theirs especially in scenarios involving remote work, geographic restrictions, and dual roles.
Security	**Certified secure environment** Data will be accessed within certified secure environments appropriate to the classification of the data, e.g. ONDC Accredited Data Service Provider, IRAP-certified or Essential 8.			✓	Not applicable as data is only accessible via PeopleWA's secure environment.
Security	**Consistent security labelling and classification**		✓		Data requesters must provide information on how they track and enforce labelling and classification procedures where they have received a sensitive approved export.

Theme	Attribute	Strong alignment	Partial alignment	Not assessed	Reasoning for alignment with attributes
	Agencies will assign appropriate security classifications for data assets and outputs to guide handling and sharing.				
Security	**Established security clearance assessments** Agencies will consistently use established security clearance/vetting process, e.g. Australian Government Security Vetting Agency.			✓	Not applicable as PeopleWA conduct vetting processes instead of requesting agency.
Security	**Incident monitoring and response mechanisms** Mechanisms for incident monitoring, identification, and response are in place.	✓			
Privacy	**Data minimisation protocols** Agencies will implement the privacy by design principle, including minimising the collection and storage of personal data to what is necessary to achieve the project, and adhering to approved retention and disposal practices.			✓	Not applicable as the PeopleWA team undertake any data minimisation and de-identification procedures. Terms and conditions of use state that requesters cannot re-identify or link the data to other sources.
Privacy	**De-identification mechanisms** Agencies will have controls and safeguards to manage re-identification risks, including removing direct identifiers, limiting access to sensitive data, using secure transfer mechanisms or controlled environments, and adhering to the separation principle.			✓	Not applicable as the PeopleWA team undertake any data minimisation and de-identification procedures. Terms and conditions of use state that requesters cannot re-identify or link the data to other sources.
Privacy	**Privacy incident reporting**	✓			PeopleWA require evidence of an agency's processes to handle data breaches.

Theme	Attribute	Strong alignment	Partial alignment	Not assessed	Reasoning for alignment with attributes
	Agencies will have established processes to report privacy incidents and data breaches and fulfil legislative responsibilities.				