DEFINITIONS

APP	Means the Australian Privacy Principles set out in the Privacy Act 1988 (Cth).
Personal Information	Means information or an opinion about an identified individual, or an individual who is reasonably identifiable.
Qualifications	Includes but is not limited to certificates, licenses, academic transcripts, and professional memberships used for employment validation.
Directions	has the same meaning as Directions Workforce Solutions Inc.
Sensitive Information	A sub-set of personal information that includes information about an individual's criminal record (Police Clearances) or biometric information.
Validation Documents	Includes but is not limited to Passports, Birth Certificates, and National Police Clearances used for onboarding and safety validation.

PURPOSE

Directions is committed to protecting the privacy of its customers, employees, and stakeholders. This policy ensures that Directions manages personal information in a lawful, fair, and transparent manner in accordance with the Privacy Act 1988 (Cth) and the Australian Privacy Principles.

SCOPE

This policy applies to all personal information collected by Directions, specifically focusing on the collection of qualifications and sensitive validation documents during employment onboarding.

POLICY STATEMENT

Collection of Personal Information

Directions only collects information reasonably necessary for its functions as a workforce solutions provider. We specifically collect:

- Qualifications: Trade certificates, academic transcripts, and licenses.
- Right to Work Evidence: Passports or Birth Certificates to verify legal entitlement to work in Australia.
- Safety & Security Data: National Police Clearances and Working with Children Checks to ensure the continuity of staffing and host company environments.
- Consent: Directions will only collect sensitive information (like criminal records) with the individual's explicit consent.

Use and Disclosure

Directions uses this information for:

- Validating the professional standing and identity of candidates.
- Meeting legal obligations under the Migration Act (Right to Work).
- Assessing suitability for specific work sites (e.g., licensed venues or schools).
- Secondary Use: We do not use sensitive information for marketing or share it with third parties unless required by law or specifically consented to for site access.

Data Security and Storage

Given the high-risk nature of identity documents (Passports) and clearances:

- Access Control: Access to validation documents is restricted to authorized HR and Payroll personnel.
- Encryption: Digital copies are stored in secure, encrypted environments.
- Retention: Directions only retains sensitive clearances for as long as required to validate the placement. Documents are securely destroyed or de-identified once their legal or business purpose has expired.

Data Breach Notification

In the event of a data breach involving sensitive information (like a passport number), Directions will comply with the Notifiable Data Breaches (NDB) scheme, notifying affected individuals and the OAIC if the breach is likely to result in serious harm.

ROLES & RESPONSIBILITIES

All employees, Board members and contractors are required to be responsible and accountable for deployment and application of this policy within their area of responsibility.

The Security and Privacy Officer is responsible for overseeing compliance. All staff involved in onboarding must ensure sensitive documents are not left in public view or unencrypted folders.

REFERENCES

Legislation:

- Privacy Act 1988 (Cth)
- Migration Act 1958 (Cth))

DOCUMENT DETAILS

This policy is to be reviewed at a minimum every three (3) years, or as required, as part of Directions' commitment to continual improvement.

Version	Action	Date	Approved by	Date	Review Due
2.0	Prepared for Approval	28/01/2026	Approved		