



Privacy Statement

Arnold Group Australia Pty Ltd trading as **Safety People Australia**
ABN: 67 007 041 358

Effective date: June 2026

1. Introduction

Arnold Group Australia Pty Ltd, trading as Safety People Australia, together with its related businesses, brands and divisions, is committed to protecting the privacy of the people we deal with, including candidates, contractors, clients, referees, suppliers, website users and other business contacts.

This Privacy Statement explains how we collect, hold, use, disclose, protect and manage personal information in accordance with the Privacy Act 1988 (Cth), the Australian Privacy Principles (APPs) and other applicable privacy, employment, recruitment and data protection obligations.

In this Privacy Statement, “we”, “us” and “our” refers to Arnold Group Australia Pty Ltd, Safety People Australia and any related trading names, divisions or business operations.

“Personal information” means information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information is true or not and whether it is recorded in a material form or not.

2. Who this Privacy Statement applies to

This Privacy Statement applies to personal information we collect and handle about:

- job applicants and candidates;
- contractors, temporary workers and placed workers;
- employees and prospective employees;
- referees and emergency contacts;
- client contacts and hiring managers;
- suppliers and service providers;
- visitors to our websites and social media pages;
- people who subscribe to our newsletters, alerts, events or market updates;
- people who contact us by phone, email, website, social media, online form or other communication channels.

3. Types of personal information we collect

The types of personal information we collect will depend on the nature of your relationship with us. This may include:

- name, address, email address, phone number and other contact details;
- employment history, resume, qualifications, licences, tickets and certifications;
- work rights, visa status and right-to-work information;
- salary expectations, availability, notice period and preferred work locations;
- interview notes, assessment results and candidate profile information;
- references, referee comments and employment verification information;
- information collected from publicly available sources, job boards, professional networks and social media platforms;
- identification documents, where required for verification, compliance, onboarding or placement purposes;
- payroll, taxation, superannuation, banking and invoicing information, where relevant;
- information about client contacts, roles, vacancies, business requirements and recruitment activity;
- website usage data, analytics information, cookies, device information and online interaction data;
- communications with us, including emails, phone records, notes, forms and messages.

4. Sensitive information

In some circumstances, we may collect sensitive information where it is reasonably necessary for our recruitment, placement, workforce management, compliance or related business functions.

Sensitive information may include:

- health information;
- injury, return-to-work or work capacity information;
- workers compensation or injury management information;
- medical assessment or functional capacity information;
- criminal history information;
- membership of professional associations or trade unions, where relevant to a role;
- information about licences, regulatory approvals, disciplinary matters or professional registrations;
- background screening, police check or pre-employment check information.

We will only collect sensitive information where:

- you have consented to the collection;
- the collection is reasonably necessary for one or more of our functions or activities;
- the collection is required or authorised by law;
- the collection is necessary for legal, regulatory, insurance, workplace health and safety, employment, recruitment or placement purposes; or
- another exception under applicable privacy laws applies.

5. How we collect personal information

We may collect personal information directly from you when you:

- apply for a role;
- submit your resume;
- register with us;
- complete an online form;
- attend an interview;
- speak with one of our consultants;
- provide documents or information to us;
- subscribe to job alerts, newsletters or market updates;
- contact us by phone, email, website, social media or other channels.

We may also collect personal information from third parties, including:

- referees;
- previous employers;
- clients and prospective employers;
- job boards and recruitment platforms, including SEEK and LinkedIn;
- publicly available sources;
- professional networks and industry contacts;
- social media platforms, where relevant to recruitment or business purposes;
- background checking, assessment, testing or verification providers;
- migration, legal, payroll, insurance, training or compliance providers;
- government, regulatory or law enforcement agencies, where required or permitted by law.

Where reasonable and practicable, we will collect personal information directly from you. However, in recruitment and executive search, we may collect information from publicly available sources or professional networks before we contact you.

6. Why we collect, use and disclose personal information

We collect, hold, use and disclose personal information for purposes connected with our business, including:

- assessing your suitability for current and future employment, contract or consulting opportunities;
- contacting you about job opportunities, market updates, career opportunities or related services;
- introducing candidates to clients and prospective employers;
- managing recruitment, search, selection, assessment and placement processes;
- verifying qualifications, employment history, licences, work rights and references;
- managing temporary, contract, labour hire or consulting placements;
- supporting onboarding, payroll, invoicing, taxation, superannuation and insurance processes;
- managing client relationships, job briefs, recruitment campaigns and service delivery;
- conducting candidate care, client care, market mapping and talent pooling;
- complying with legal, regulatory, contractual, workplace health and safety, employment, taxation and insurance obligations;
- responding to enquiries, complaints, access requests or privacy matters;
- improving our services, systems, website, communications and business processes;
- sending newsletters, event invitations, job alerts, industry insights and marketing communications, where permitted by law;
- protecting our legal rights, managing disputes, investigating incidents and maintaining records;
- using technology, automation and business systems to improve recruitment and administrative processes.

We will not use or disclose your personal information for a purpose unrelated to the purpose for which it was collected unless you have consented, you would reasonably expect us to do so, or we are otherwise permitted or required by law.

7. Candidate information and recruitment activities

As a recruitment and workforce services business, we may collect, use and disclose candidate information for current and future opportunities.

If you provide us with your resume or candidate details, we may retain that information so we can contact you about suitable roles in the future, unless you ask us not to do so.

We may disclose candidate information to clients, prospective employers, hiring managers, assessment providers, background checking providers, referees, payroll providers, insurance providers and other parties involved in recruitment, assessment, placement, onboarding, workforce management or compliance processes.

We will take reasonable steps to ensure candidate information is accurate, up to date and relevant before it is presented to a client or prospective employer.

8. Referees

If you provide details of a referee, you should ensure the referee has agreed to be contacted by us.

We may collect information from referees about your employment history, performance, conduct, skills, experience, suitability and other matters relevant to recruitment or placement decisions.

We will use referee information for recruitment, assessment, verification and related business purposes.

9. Direct marketing and communications

We may use your personal information to send you information about job opportunities, market updates, events, newsletters, surveys, services or other information that may be relevant to you.

We will only send marketing communications where permitted by law.

You can opt out of receiving marketing communications at any time by using the unsubscribe function in our emails or by contacting us directly.

Even if you opt out of marketing communications, we may still contact you about active recruitment processes, placements, contractual matters, compliance issues, service updates or other non-marketing communications.

10. Website, cookies and analytics

When you visit our website, we may collect information such as:

- IP address;
- browser type;
- device information;
- pages visited;
- time spent on the website;
- referral source;
- online interactions;
- cookies and analytics data.

We use this information to improve our website, understand user behaviour, maintain website security, support marketing activities and improve our services.

You may be able to disable cookies through your browser settings. However, some website features may not function properly if cookies are disabled.

Our website may contain links to third-party websites, platforms or services. We are not responsible for the privacy practices, content or security of those third-party websites.

11. Social media

If you interact with us through social media platforms, we may collect information that you provide or make available through those platforms.

Social media platforms are operated by third parties and have their own privacy policies and data handling practices. You should review the privacy settings and policies of any social media platform you use.

12. Use of technology, automation and artificial intelligence

We may use technology, automation, artificial intelligence, database tools and workflow systems to assist with:

- recruitment administration;
- candidate search and matching;
- database management;
- communication management;
- job alert distribution;
- screening support;
- document handling;

- workflow automation;
- reporting and business improvement.

We do not rely solely on automated systems to make final recruitment, placement or employment decisions that significantly affect candidates. Human review remains part of our recruitment and assessment process.

Where automated tools are used to assist with decisions that may affect rights or interests, we will take reasonable steps to be transparent about the kinds of personal information used and the kinds of decisions or recommendations supported by those tools.

13. Disclosure of personal information

We may disclose personal information to:

- clients and prospective employers;
- hiring managers and recruitment decision-makers;
- referees and previous employers;
- background checking, assessment, testing or verification providers;
- payroll, accounting, superannuation, taxation and banking providers;
- insurance providers, legal advisers, auditors and professional advisers;
- technology, cloud hosting, software, database, communications and IT support providers;
- marketing, survey, event and email communication providers;
- training, compliance, medical, occupational health or workplace health and safety providers;
- government, regulatory, law enforcement or statutory bodies, where required or permitted by law;
- related bodies corporate, business partners, contractors or service providers who assist us in operating our business.

We require service providers who handle personal information on our behalf to take reasonable steps to protect that information and use it only for authorised purposes.

14. Overseas disclosure

Some of our service providers, platforms or technology systems may store, process, access or transmit personal information outside Australia.

This may occur through cloud-based recruitment systems, email platforms, job boards, communication tools, analytics providers, automation tools, artificial intelligence tools, background checking providers, software providers, IT support services and other technology platforms.

The countries in which overseas recipients are located may vary depending on the systems and providers we use from time to time. Where practicable, we will take reasonable steps to identify the countries in which overseas recipients are likely to be located and to ensure overseas recipients handle personal information consistently with the Australian Privacy Principles.

15. Security of personal information

We take reasonable steps to protect personal information from misuse, interference, loss, unauthorised access, modification or disclosure.

These steps may include:

- secure technology systems;
- password protection and access controls;
- staff training and confidentiality obligations;
- secure document storage;
- system monitoring and security controls;
- limiting access to personal information to those who need it for business purposes;
- using reputable technology and service providers;

- reviewing and improving our privacy and data handling practices.

No method of transmission or storage is completely secure. However, we take privacy and data security seriously and work to manage these risks appropriately.

16. Notifiable data breaches

If we become aware of a suspected or actual data breach involving personal information, we will take reasonable steps to contain, assess and respond to the incident.

Where required under the Notifiable Data Breaches scheme, we will notify affected individuals and the Office of the Australian Information Commissioner if the breach is likely to result in serious harm.

We will also take reasonable steps to reduce the risk of similar incidents occurring in the future.

17. Retention and destruction of personal information

We retain personal information for as long as reasonably necessary for the purposes for which it was collected, including recruitment, placement, client management, legal, insurance, taxation, audit, dispute resolution and compliance purposes.

Candidate information may be retained so we can contact candidates about future opportunities, unless they ask us to delete or de-identify their information and we are legally able to do so.

When personal information is no longer required, we will take reasonable steps to destroy or de-identify it, unless we are required or permitted by law to retain it.

18. Accessing your personal information

You may request access to personal information we hold about you.

We will respond to access requests within a reasonable period. We may need to verify your identity before providing access.

In some circumstances, we may refuse access or provide limited access where permitted by law, including where providing access would:

- unreasonably affect the privacy of others;
- prejudice legal proceedings, investigations or negotiations;
- reveal commercially sensitive information;
- be unlawful;
- be otherwise permitted to be refused under applicable privacy laws.

If we refuse access, we will explain the reason where it is reasonable and lawful to do so.

19. Correcting your personal information

We take reasonable steps to ensure the personal information we hold is accurate, complete, up to date and relevant.

You may ask us to correct personal information we hold about you if you believe it is inaccurate, out of date, incomplete, irrelevant or misleading.

If we agree that the information should be corrected, we will take reasonable steps to correct it. If we do not agree, you may ask us to attach a statement to the information noting that you believe it is inaccurate, out of date, incomplete, irrelevant or misleading.

20. Anonymity and pseudonymity

Where lawful and practicable, you may deal with us anonymously or by using a pseudonym.

However, in many recruitment, placement, verification, compliance, payroll and client service situations, it may not be practicable for us to deal with you anonymously or under a pseudonym.

21. Complaints

If you have a concern or complaint about how we have handled your personal information, you can contact us using the details below.

Please provide enough information for us to understand and investigate your concern.

We will acknowledge your complaint and aim to respond within a reasonable period, usually within 30 days.

If you are not satisfied with our response, you may contact the Office of the Australian Information Commissioner.

22. Contact us

For privacy enquiries, access requests, correction requests or complaints, please contact:

Privacy Officer

Arnold Group Australia Pty Ltd trading as Safety People Australia

Email: enquiries@arnoldgroup.com.au

Phone: 1300 28 00 68

23. Changes to this Privacy Statement

We may update this Privacy Statement from time to time to reflect changes in our business, technology, systems, legal obligations or privacy practices.