PRIVACY POLICY

Purpose

We help our customers into employment and to do this we need to ask for and use Personal Information. We take the privacy of our customers, team members, volunteers, contractors, and all other people who we deal with seriously. We do what's right and keep Personal Information and Sensitive Information safe and secure.

It is your responsibility to check this Privacy Policy periodically for changes. If we adopt a new Privacy Policy, we will post the new Privacy Policy on our website and intranet, and it will then apply through your acceptance of it by subsequent or continued use of the website and/or Campbell Page's services.

Scope

This Privacy Policy applies to any person that Campbell Page Limited and its Related Bodies Corporate may deal with from time to time including, but not limited to, customers, clients, and participants, as well as Campbell Page team members and our contractors and volunteers.

Team members, volunteers and contractors of Campbell Page and its Related Bodies Corporate should note that we must comply with the additional requirements under government privacy policies regarding how we deal with personal information, in addition to those set out in this Privacy Policy.

Policy Statement

This Privacy Policy describes Campbell Page's requirements against the Australian Privacy Principles and how we collect and use Personal Information and Sensitive Information.

'Personal Information' is information or an opinion about an identified individual, or an individual who is reasonably identifiable. Examples of personal information include an individual's name, signature, address, telephone number, date of birth, bank account details, employment details and commentary or opinion about an individual.

'Sensitive Information' is sensitive information about an individual and is a subset or type of Personal Information. Examples of sensitive information include information about an individual's racial or ethnic origin, information or an opinion about an individual's criminal record or health information about an individual.

The definitions used in this Privacy Policy are described in the 'Definitions' section below.

What information we collect

Personal Information we collect about you may include identification information such as your name, address, email address, phone number(s), passport details, immigration status, financial and payment information, and such other information necessary and/or convenient for delivering our services.

We also collect Technical Data through 'cookie' technology on our webpage. This information is used to enhance the usability and functionality of our website and for marketing, advertising, and analytic purposes.

We will only collect or hold any Sensitive Information about you with your consent or if you volunteer such Sensitive Information to us. If we collect or hold your Sensitive Information in accordance with this section, we may disclose such sensitive information to our Related Bodies Corporate.

Why we collect information

We collect Personal Information from you and you consent to us using your Personal Information (other than Sensitive Information) for the following Primary and Secondary Purposes:

- to process and deliver services including, but not limited to, those set out in any applicable contractual documents
- if you are seeking employment:
  - to assist you with career guidance and work placements

- to provide you information about possible work opportunities
- to comply with applicable health and safety obligations
- to inform you about training programs
- to help us assess an application submitted by you or on your behalf in relation to your employment with us or one of our clients

- If you are seeking employment or are our client:
  - to personalise and customise your experiences with us
  - to help us meet our contractual and service obligations
  - to help us review, manage and enhance our services and develop insights used in reports or other content developed by us
  - to offer additional benefits to clients
  - to communicate with you, including by email, mobile and via our website;
  - to investigate any complaints about or made by you, or if we have reason to suspect you have breached any relevant terms
  - to outsource a number of services to third party suppliers (including software solution providers, superannuation fund managers, background checking and screening agents)
  - to do anything else as required or permitted by any law

We will not collect Personal Information unless the information is reasonably necessary for, or directly related to, one or more of our functions or activities. We will also obtain consent prior to collecting any Sensitive Information and will only do so if the information is reasonably necessary for one or more of our functions or activities.

How we collect information

How we collect information is dependent on the services we are providing to our customers. This can include information provided by our funders, forms, email, social media, or verbal interactions.

There are many ways we collect information that we hold. We collect information when:

- forms are completed
- when we receive or make calls
- when we receive emails or enquiries through our website
- when our customers visit our website or attend one of our sites
- we receive a referral through the government

We validate the Personal Information we collect from you with information about you that has been submitted to government agencies, to which we have been provided access.

Storing Information

We store information electronically and on paper. We also use Cloud technology to store data safely.

In relation to all Personal Information, we will take all reasonable steps to:

- ensure that the Personal Information we collect is accurate, up to date and complete
- ensure that the Personal Information we hold, use or disclose is, with regard to the relevant purpose, accurate, up to date, complete and relevant
- protect Personal Information from misuse, loss or unauthorised access and disclosure

We only store information for as long as legally required.

Use and Disclosure of Information

We will only use your Personal Information for the purposes for which are related to the Primary and Secondary Purposes, and to conduct research on how we can improve our services, either internally or through subcontractors.

Sometimes we need to share Personal Information with other entities. The Privacy Act and Australian Privacy Principles set out what we can and can't do with that information. We may need to disclose Personal Information to:

- a government authority, law enforcement agency, or pursuant to a court order
- allow us to provide you with our services
- third party service providers who perform functions, or provide services on our behalf
- facilitate the provision of services requested by you by third parties
- our Related Bodies Corporate
- a party of a transaction involving the sale of our business or its assets
- our professional advisors, including our accountants, auditors, and lawyers, or
- otherwise as required by law

When we use or share your personal information, we always follow our values and 'Do What's Right'. This means we apply the 13 Australian Privacy Principles, and we do what the law tell us to do.

In circumstances when we share information to third parties to provide you services or we use third party software providers to store information (e.g. Microsoft), your Personal Information may be transferred overseas, including to the United States. Where reasonably practicable, we will provide you with notice and seek your consent to the transfer of your Personal Information overseas.

There are certain provisions in the Social Security (Administration) Act 1999 that enables the disclosure of protected information in some circumstances including where a Public Interest Certificate has been issued.

In the event of an emergency, we may need to disclose information to services such as police, ambulance, fire service, State Emergency Service officers, emergency call service operators, health service providers and child protection agencies.

Marketing Material

We may contact you with marketing material if:

- we collected the information from you
- it is reasonable in the circumstances to expect that we would use or disclose the information for direct marketing purposes
- we provide you with a simple means to 'opt-out' of direct marketing communications from us
- you have not elected to 'opt-out' from receiving such direct marketing communications from us

You can tell us if you don't want to receive marketing material (opt-out) by using our contact details set out in the 'Contact Details and Feedback' section below or contacting us via our website.

Your Right to refuse collection, use or disclosure

You have the right to refuse consent to the collection, use or disclosure of your Personal Information or Sensitive Information. Please note, however, that this will restrict the services we can provide to you.

If you would like to access any of our products and services on an anonymous or pseudonymous basis, we will take reasonable steps to comply with your request, however:

- you may be precluded from taking advantage of some or all of our products and services, and
- we will require you to identify yourself if:
  - we are required by law to deal with individuals who have identified themselves, or
  - it is impracticable for us to deal with you if you do not identify yourself

Privacy Breaches

A data breach occurs when:

- there is unauthorised access to or disclosure of Personal Information held by us, or
- Personal Information is lost in circumstance where unauthorised access or disclosure is likely to occur, and
- it is likely to result in serious harm to any of the individuals to whom the information relates, and
- we have been unable to prevent the likely risk of serious harm with remedial action.

Any potential breaches are assessed promptly by the Campbell Page Contract Assurance Team.

Access and Correction

Access

If you require access to your personal information, please contact us using our contact details set out below. You may be required to put your request in writing and provide proof of identity.

We are not obliged to allow access to your personal information if one of the circumstances outlined in APP 12.3 applies.

If you make a request for access to personal information, we will

- respond to your request within a reasonable period after the request is made, and
- if reasonable and practicable, give access to the personal information as requested

If we refuse to give access to the personal information, we will give you a written notice that sets out at a minimum:

- our reasons for the refusal (to the extent it is reasonable to do so), and
- the mechanisms available to complain about the refusal

Correction

We request that you keep your personal information as current as possible. If you feel that information about you is not accurate or your details have or are about to change, you can contact us using our contact details set out below and we will correct or update your personal information.

If you otherwise make a request for us to correct your personal information, we will:

- respond to your request within a reasonable period after the request is made, and
- if reasonable and practicable, correct the information as requested

  If we refuse a request to correct personal information, we will:

- give you a written notice setting out the reasons for the refusal and how you may make a complaint, and
- take reasonable steps to include a note with your personal information of the fact that we refused to correct it

Complaints

If you have a complaint about how we collect, use, disclose, manage, or protect your personal information, or consider that we have breached the Privacy Act or APPs, please contact us using our contact details below. We will respond to your complaint within 14 days of receiving the complaint.

Once the complaint has been received, we may resolve the matter in a number of ways:

- We may request further information from you. Please provide us with as much information as possible, including details of any relevant dates and documentation. This will enable us to investigate the complaint and determine an appropriate solution

- We will discuss options for resolution with you and if you have suggestions about how the matter might be resolved you should raise these with our Privacy Officer
- Where necessary, the complaint will be investigated. We will try to do so within a reasonable time frame. It may be necessary to contact others in order to proceed with the investigation. This may be necessary in order to progress your complaint
- If your complaint involves the conduct of our employees, we will raise the matter with the employees concerned and seek their comment and input in the resolution of the complaint
- After investigating the complaint, we will give you a written notice about our decision
- You are free to lodge a complaint directly with the OAIC online, by mail, fax, or email. For more information please visit the OAIC website at https://www.oaic.gov.au/

Responsibilities

Compliance, monitoring and review

- All staff are responsible for adhering to privacy requirements in relation to our customer's Personal Information and Sensitive Information
- All staff are responsible for adhering to the internal procedures and workflows for their relevant program in relation to customer privacy, requests for information, Class PIC's and Data Breaches
- Contract Assurance Team are responsible for updating workflows and procedures for DES and ParentsNext in accordance with any updated Guidelines released by funders

Reporting

All staff are required to contact Campbell Page's Contract Assurance Team in relation to any privacy enquiries, potential privacy and data breaches, information requests and PIC's.

Records Management

Staff must maintain all records relevant to administering this policy in a recognised Campbell Page record keeping system.

Contact Details & Feedback

You may contact us in relation to this Privacy Policy by emailing:

Kylie Van Der Neut
Senior Manager of Contract Assurance / Privacy Officer
ES-Quality-Team@campbellpage.org.au

Campbell Page staff may provide feedback about this document by emailing policy@campbellpage.org.au or contacting the Policy Sponsor.

Definitions

Definitions and Acronyms	
Australian Privacy Principles or **APPs**	The Australian Privacy Principles as set out in Schedule 1 of the Privacy Act
Data Breach	Occurs when Personal Information that an entity holds is subject to unauthorised access or disclosure, or is lost
FOI Act	Freedom of Information Act 1982 (Cth) as amended from time to time
Personal Information	Has the meaning given in the Privacy Act
PIC	Public Interest Certificate

Primary and Secondary Purposes	The Primary and Secondary purposes listed in the 'Why we collect information' section of this Privacy Policy
Privacy Act	Privacy Act 1988 (Cth) as amended from time to time
Related Bodies Corporate	Has the meaning given to that term in section 50 of the Corporations Act 2001 (Cth)
Sensitive Information	Has the meaning given in the Privacy Act
Technical Data	• The Internet protocol (IP) address or MAC address used to connect your computer to the Internet, your login information, browser type and version, time zone setting, browser plug-in types and versions, operating system and platform, and • Information about your visit to our website, such as the full Uniform Resource Locators (URL), clickstream to, through and from our website (including date and time), services viewed or searched for, page response times, download errors, length of visits to certain pages, page interaction information (such as scrolling, clicks, and mouse-overs) and methods used to browse away from a page

Related legislation and documents

Supporting Information	
Legislative Compliance	This Policy supports Campbell Page's compliance with the following legislation: • Privacy Act 1988 (Cth) • Privacy and Personal Information Protection Act 1998 (NSW) • Social Security (Administration) Act 1999 • Health Records and Information Privacy Act 2002 (NSW) • Privacy and Data Protection Act 2014 (VIC) • Health Records Act 2001 (Vic) • The Queensland Information Privacy Act (2009) • Queensland Health Quality and Complaints Commission Act 2006 (Qld) • State Records Act 1997 (SA)
Supporting Documents	Privacy Guideline – ParentsNext Privacy Guideline – DES
Related Documents	Release of Information in an Emergency - ParentsNext Release of Information in an Emergency – DES Notifiable Data Breach Policy
Superseded Documents	Privacy Policy, created 3.0 30/01/2023

Approval and Review Details

Revision History				
Version	**Policy Sponsor**	**Approval Team**	**Approval/Effective date**	**Next review**
5.0	Contract & Compliance	Campbell Page Board	February 2024	February 2026
Sections Modified	V5.0 Update to Legislative Compliance - Removal of refence to jobactive - Fix of broken links			