

PRIVACY POLICY

1. Introduction

1.1 APP Entity

PJ Maynard Consulting Pty Ltd® manages personal information, as an APP Entity, under the Australian Privacy Principles (APPs).

1.2 Information Flow

When we collect your personal information:

- We check that it is reasonably necessary for our recruitment process [3: *Purposes*] as an employment agency;
- We check that it is current, complete and accurate. This will sometimes mean that we have to cross check the information that we collect from you with third parties;
- We record and hold your information in our HighRise 37 signals database [5: *How your personal information is held*]. Some information may be disclosed to HighRise 37 signals in the USA and Microsoft Office 365.
- We retrieve your information when we need to use or disclose it for our recruitment process [3: *Purposes*]. At that time, we check that it is current, complete, accurate and relevant. This will sometimes mean that we have to cross check the information that we collect from you with third parties once again - especially if some time has passed since we last checked.
- Subject to some exceptions, we permit you to access [7: *Access & Correction*] your personal information in accordance with APP:12 of the (APPs).
- We correct or attach associated statements to [7: *Access & Correction*] your personal information in accordance with APP:13 of the (APPs).
- We destroy or de-identify your personal information when it is no longer needed for any purpose [3: *Purposes*] for which it may be used or disclosed provided that it is lawful for us to do so. We do not destroy or de-identify information that is contained in a Commonwealth Record.

2. Kinds of information that we collect and hold

2.1 For Work seekers

The type of information that we typically collect and hold about Work seekers is information that is necessary to assess amenability to work offers and work availability;

suitability for placements; or to manage the performance in work obtained through us and includes:

- Employment experience
- Education and qualifications
- Contact details
- Conversation logs
- Location of desired job / work
- Salary
- Job preferences

2.2 For Clients

The type of information that we typically collect and hold about Clients is information that is necessary to help us manage the presentation and delivery of our services and includes:

- Contact details
- Company and employee details
- Job descriptions
- Conversation logs
- Billing details and records
- Recruitment agreements

2.3 For Referees

The type of information that we typically collect and hold about Referees is information that is necessary to help to make determinations about the suitability of one of our Work seekers for particular jobs or particular types of work and includes:

- Contact details
- Referee employment experience and relationship to work seeker
- Reference check

3. Purposes

3.1 For Work seekers

Information that we collect, hold, use and disclose about Work seekers is typically used for:

- Work placement operations;
- Recruitment functions;
- Statistical purposes and statutory compliance requirements;
- Client requests for contact details;
- Service standard surveys post-recruitment functions

- Direct marketing of work seeker to client (with work seeker permission)

3.2 For Clients

Personal information that we collect, hold, use and disclose about Clients is typically used for:

- Client and business relationship management;
- Recruitment functions;
- Marketing services to you;
- Statistical purposes and statutory compliance requirements;
- Service standard surveys post-recruitment functions

3.3 For Referees

Personal information that we collect, hold, use and disclose about Referees is typically used for:

- To confirm identity and authority to provide references;
- Work seeker suitability assessment and comment;
- Validation of work seeker provided information
- Recruitment functions;

3.4 Our Policy on Direct Marketing

PJ Maynard Consulting Pty Ltd® may use personal information to email or post marketing newsletters through Microsoft email exchange.

- Contact details obtained from Highrise Database
- Individuals have the option to unsubscribe
- No third party will have access to your details

4. How your personal information is collected

4.1 For Work seekers

Personal information will be collected from you directly when you forward your resume or any other information in connection with your application to us for work.

We may also collect personal information about you from a range of publicly available sources including newspapers, journals, directories, the Internet and social media sites. When we collect personal information about you from publicly available sources for inclusion in our records we will manage the information in accordance with the [APPs](#) and our Privacy Policy.

4.2 For Clients

Personal information about you may be collected:

- When you provide it to us for business or business related social purposes;
- We may also collect personal information about you from a range of publicly available sources including newspapers, journals, directories, the Internet and social media sites. When we collect personal information about you from publicly available sources for inclusion in our records we will manage the information in accordance with the APPs.

4.3 For Referees

Personal information about you may be collected when you provide it to us, or when your contact details are provided to us by Work Seekers:

- In the course of our checking Work seeker references with you and when we are checking information that we obtain from you about Work seekers;
- We may also collect personal information about you from a range of publicly available sources including newspapers, journals, directories, the Internet and social media sites. When we collect personal information about you from

publicly available sources for inclusion in our records we will manage the information in accordance with the APPs.

4.4 Photos and Images

We will not request that you supply photographs, scan photo ID, or capture and retain video image data of you in cases where simply sighting photographs or proof of identity documents would be sufficient in the circumstances.

We will request a photo for our database, which can be accepted or declined by you.

4.5 Electronic Transactions

- *Social Networks & Web Searches;*

LinkedIn, Facebook, Twitter, Google, Instagram.

- *Resume Harvesting and Job Matching;*

Ms Office, LinkedIn, HighRise 37 signals database.

- *Web Browsing;*

Technical terms / definitions

A web browser is software that allows a user to access and view web pages. Examples are Microsoft Internet Explorer, Netscape Navigator, Firefox and Opera.

Technical details in relation to visits to this website are logged by our internet service provider for statistical purposes.

The technical details logged are confined to the following items:

- The type of web browser and operating system used to access our site;
- The Internet domain name used;
- The IP address of the visitor's web server;
- The date and time you access our site and visit duration;
- Clickstream data which shows the traffic of visitors around this web site (for example, pages accessed and documents downloaded)
- Some of the search criteria that you are using.

No information is collected that could be used to identify individual website visitors. For example, we may count the number of visitors to the different pages of our

website to help make them more useful to visitors. This information does not identify you personally.

Some of the above information is used to create summary statistics which allow us to assess the number of visitors to the different sections of our site, discover what information is accessed most frequently, inform us on future design and layout specifications, and help us make our site more user friendly.

This site uses [Google Analytics](#), Custom Search and Maps services provided by Google, Inc. ("Google"). Google uses "cookies", which are text files placed on your computer, to help the website analyse how users use the site. The information generated by the cookie about your use of the website (including your IP address) will be transmitted to and stored by Google on servers in the United States. Google will use this information for the purpose of evaluating your use of the website, compiling reports on website activity for website operators and providing other services relating to website activity and internet usage. Google may also transfer this information to third parties where required to do so by law, or where such third parties process the information on Google's behalf. Google will not associate your IP address with any other data held by Google. You may refuse the use of cookies by selecting the appropriate settings on your browser, however please note that if you do this you may not be able to use the full functionality of this website. By using this website, you consent to the processing of data about you by Google in the manner and for the purposes set out above.

- *Cookies;*

We may also collect anonymous information through the use of cookies on our website. Cookies are pieces of information that are stored on your computer's hard disk. Most web-browsers are set to accept cookies but you can set your web-browser to refuse cookies. Cookies themselves do not identify users personally but they do allow the tracking of an individual's use of a website. Cookies have become commonplace. You

can configure your web browser to reject or accept cookies. If you reject cookies you may not be able to interact with us online.

- Web Bugs;

We may occasionally embed an object into a web page or email, through WordPress or Microsoft Outlook, to monitor website traffic and receive email receipt confirmation. This is for internal purposes only.

- Cloud Computing Services;

In cases where we use cloud computing services we will take reasonable steps to ensure that;

- Disclosure of your personal information to the cloud service provider is consistent with our disclosure obligations under the AAPs. This may include ensuring that we have obtained your consent, or that the disclosure is for purposes within your reasonable expectations.
- Disclosure is consistent with any other legal obligations, such as the restrictions on the disclosure of tax file number information or the disclosure by private employment agencies of work seeker details.
- Our cloud computing services provider's terms of service recognises that we are bound by obligations to protect the privacy of your personal information and that they will not do anything that would cause us to breach those obligations.

- Uploading Photographs;

If you are a Work Seeker and are interviewed or met with face to face, you may be asked if we can take a photograph and collect and store this on our HighRise 37 signals database. If you verbally accept this, you agree for us to collect and store this photograph purely for PJ Maynard Consulting Pty Ltd reference. Your photograph isn't ever forwarded to a third party.

- Emails;

If we receive an email from you on occasion, particularly if you are a Work Seeker or Client, we will collect this email on our HighRise 37 signals database and on Microsoft Office 365 - SharePoint. This is stored for future reference and context in a recruitment process.

- Call & Message Logs;

If we call you, as a Work Seeker, Referee or Client, often we collect and record the content and general gist of our conversation on our HighRise 37 signals database. This is stored for future reference, or for job matching if you are a Work Seeker.

- Teleconference & Video Conferences;

We use FaceTime, Skype and Lync for video conferencing purposes on occasion.

- Database;

HighRise 37 signals database.

- Mobile Access;

We do not use mobile web apps widely. We may use HighRise 37 signals mobile app for easy access of personal information that we may have collected about you if you are a job seeker or client.

- Paperless Office;

PJ Maynard Consulting is a 'paperless' office. This means that wherever possible, we use soft copy of documents ([MS Office 365](#)), save documents received by email electronically, and so minimising paper flow through the office. This minimises the risk of your personal information being viewed or accessed by another party.

5. How personal information is held

5.1 Our Information Record System

Personal information is held in our HighRise 37 signals Database [*5.1: Information Record System*] until it is no longer needed for any purpose for which it may be used or disclosed at which time it will be de-identified or destroyed provided that it is lawful for us to do so.

We take a range of measures [*5.2: Information Security*] to protect your personal information from:

- misuse, interference and loss; and
- Unauthorised access, modification or disclosure.

5.2 Information Security

PJ Maynard Consulting Pty Ltd® trains all staff and consultants on the use of technology for collection, storage and distribution of personal information. They adhere to our Privacy Policy.

Staff training

- "Clean desk" procedures
- Need-to-know and authorisation policies
- Just-in-time collection policies
- Password protection
- Policies on laptop, mobile phone and portable storage device security;
- Policy on timely culling
- Culling procedures including shredding and secure disposal etc.

6. Disclosures

We may disclose your personal information for any of the purposes [3: *Purposes*] for which it is primarily held or for a lawful related purpose [6.1: *Related Purpose Disclosures*].

We may disclose your personal information where we are under a legal duty to do so.

Disclosure will usually be:

- Internally
- To our related entities and consultants
- To our Clients
- To Referees for suitability and screening purposes.

6.1 Related Purpose Disclosures

We outsource a number of services to contracted service suppliers (CSPs) from time to time. Our CSPs may see some of your personal information. Typically our CSPs would include:

- Software solutions providers;
- I.T. contractors and database designers and Internet service suppliers;
- Recruitment administrative;
- Legal and other professional advisors;
- Insurance brokers, loss assessors and underwriters;
- Superannuation fund managers;
- Background checking and screening agents;
- Psychologists who perform psychometric testing on work seekers

We take reasonable steps to ensure that terms of service with our CSPs recognise that we are bound by obligations to protect the privacy of your personal information and that they will not do anything that would cause us to breach those obligations.

6.2 Cross-Border Disclosures

Some of your personal information is likely to be disclosed to overseas recipients. We cannot guarantee that any recipient of your personal information will protect it to the standard to which it ought to be protected. The costs and difficulties of enforcement of privacy rights in foreign jurisdictions and the impracticability of attempting to enforce such rights in some jurisdictions will mean that in some instances, we will need to seek your consent to disclosure.

The likely countries, type of information disclosed and recipients are indicated, so far as is practicable, in the following table:

Table

Country	Type of Information	Likely Recipients
USA	All personal data stored on our cloud based database system, located in USA	Highrise 37 signals IT Personnel and Contractors of our technology providers who may access data for maintenance and software upgrade purposes
USA	All personal data held by us	MS Office 365 IT Personnel and Contractors of our technology providers who may access data for maintenance, support and software upgrade purposes
India	All personal data held by us	External consultants

7. Access and Correction

7.1 Access

If you wish to obtain access to your personal information you should contact our Privacy Co-ordinator. You will need to be in a position to verify your identity.

- We charge \$75 + GST for access of personal information
- We require 30 business working days for disclosure of personal information

7.2 Correction

If you find that personal information that we hold about you is inaccurate, out of date, incomplete, irrelevant or misleading, you can ask us to correct it by [contacting us](#).

We will take such steps as are reasonable in the circumstances to correct that information to ensure that, having regard to the purpose [3: Purposes] for which it is held, the information is accurate, up to date, complete, relevant and not misleading.

If we have disclosed personal information about you that is inaccurate, out of date, incomplete, irrelevant or misleading, you can ask us to notify the third parties to whom we made the disclosure and we will take such steps (if any) as are reasonable in the circumstances to give that notification unless it is impracticable or unlawful to do so.

We will endeavour to correct any inaccurate, out of date, incomplete or irrelevant or misleading personal information disclosed about you within a reasonable timeframe (no longer than 10 working days).

If we refuse to correct personal information about you upon your request, and you wish to make a complaint you may go to *[8.1. Complaints Procedure]*.

8. Complaints

8.1 Complaints Procedure

If you are making a complaint about our handling of your personal information, it should first be made to us in writing.

You can make complaints about our handling of your personal information to our Privacy Co-ordinator Peta-Jane Maynard, phone 02 8084 2681, or email admin@pjconsulting.com.au.

You can also make complaints to the [Office of the Australian Information Commissioner](#).

Complaints may also be made to [RCSA](#), the industry association of which we are a member.

RCSA administers a Code of Conduct for the professional and ethical conduct of its members.

The RCSA Code is supported by rules for the resolution of disputes involving members.

NOTE: The Association Code and Dispute Resolution Rules do NOT constitute a recognised external dispute resolution scheme for the purposes of the APPs; but are primarily designed to regulate the good conduct of the Associations members.

When we receive your complaint:

- We will take steps to confirm the authenticity of the complaint and the contact details provided to us to ensure that we are responding to you or to a person whom you have authorised to receive information about your complaint;
- Upon confirmation we will write to you to acknowledge receipt and to confirm that we are handling your complaint in accordance with our policy.
- We may ask for clarification of certain aspects of the complaint and for further detail;
- We will consider the complaint and may make inquiries of people who can assist us to established what has happened and why;
- We will require a reasonable time (usually 30 days) to respond;

- If the complaint can be resolved by procedures for access and correction [7: Access & Correction] we will suggest these to you as possible solutions;
- If we believe that your complaint may be capable of some other solution we will suggest that solution to you, on a confidential and without prejudice basis in our response;

If the complaint cannot be resolved by means that we propose in our response, we will suggest that you take your complaint to any recognised external dispute resolution scheme to which we belong or to the Office of the Australian Information Commissioner.