Privacy Policy

We take your privacy very seriously. As part of our compliance with the Australian Privacy Principles (APP) in Australia & Information Privacy Principles (IPP) in New Zealand, Onten, requests you read the following information regarding how we collect your personal and sensitive information (sensitive information relates to Australia only) and how we maintain, use, store and disclosure of your personal and sensitive information in connection with your possible or actual work placements and sign where indicated to acknowledge your acceptance and understanding of this information.

Privacy Principles

- For Information subject to Australian law, the **National Privacy Principles** established by the Privacy Act 1988 (C'th)
- For information subject to New Zealand law, the **Personal Privacy Information Principles** established by the Privacy Act 1993 (NZ)

Necessary

We will only collect information that is necessary for the proper performance of our tasks or functions.

We do not collect personal information just because we think it could be useful at some future stage if we have no present need for it.

We do not routinely conduct criminal history checks and only do so to obtain relevant criminal history about jobs you are offered or for which you are shortlisted.

We do not collect or use personal information for the purposes of unlawful discrimination.

We may decline to collect unsolicited personal information from or about you and may take such measures as we think appropriate to purge it from our systems.

Type of Personal Information Held

Personal information that we collect and hold usually falls into the following categories:

- Candidate information submitted and obtained from the candidate and other sources in connection with applications for work;
- Work performance information;
- Information about incidents in the workplace;
- Staff information;
- Information submitted and obtained in relation to absences from work due to leave, illness or other causes;
- Information obtained to assist in managing client and business relationships;

Sensitive information (Australia only)

Sensitive information is a special category of personal information under the Australian Act. It is information or opinion about you, including membership of a professional or trade association or

membership of a trade union; criminal record; health information, racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, or sexual preferences or practices. As outlined in the Australian Act, sensitive information can, in most cases, only be disclosed with your consent.

How your information will be collected
Personal information will be collected from you directly when you fill out and submit one of our application forms or any other information in connection with your application for work.

Personal information is also collected when:

- we receive or give any reference about you;
- we receive results of inquiries that we might make of your former employers, work colleagues, professional associations or registration body;
- we receive the results of any competency or medical test or background checks including credit and criminal record checks;
- we receive performance feedback (whether positive or negative);
- we receive any complaint from or about you in the workplace;
- we receive any information about a workplace accident in which you are involved;
- we receive any information about any insurance investigation, litigation, registration or professional disciplinary matter, criminal matter, inquest or inquiry in which you are involved;
- you provide us with any additional information about you;
- electronically through our telecommunications and technology systems – see the section in this policy on electronic transactions;

Purposes for which we hold personal information
We primarily hold personal information for the following:

- Employment placement operations;
- Recruitment;
- Staff management;
- Risk management and training;
- Client and business relationship management;
- Marketing services to you; but only where this is permitted and whilst you are registered with us;
- Statistical purposes and statutory compliance requirements;

Disclosures
We may disclose your personal information for any of the purposes for which it is primarily held or for a related purpose where lawfully permitted.

We may disclose your personal information where we are under a legal duty to do so, including circumstances where we are under a contractual or lawful duty of care to disclose information.

We do not share personal information about you with government agencies, organisations or anyone else unless one of the following applies:

- You have consented;
- You would reasonably expect, or have been told, that information of that kind is usually passed to those individuals, bodies or agencies;
- it is required or authorised by law;
- it will prevent or lessen a serious and imminent threat to somebody's life or health;
- the disclosure is reasonably necessary for the enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of public revenue.

Outsourced Service Suppliers

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

- I.T. contractors and database designers and service internet service suppliers, some of whom may be off shore;
- Legal and other professional advisors;
- Insurers, loss assessors and underwriters;
- Background checking and screening agents;

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

Personal Information Quality

We take such steps as are reasonable in the circumstances to ensure that the personal information we hold and discloses is accurate, up to date, complete, relevant and not misleading. We recognise that information changes frequently with changes of address and other personal circumstances. We rely on you to tell us when there are changes to your personal information that we hold about you.

Personal Information Security

We take reasonable steps to destroy or permanently de-identify personal information when it is no longer required for any purpose for which it may be used or disclosed. However, it is not always practicable to destroy or de-identify electronic data. Where it is not reasonable to destroy or permanently de-identify personal information in electronic form, we will take reasonable steps to prevent inadvertent access to it.

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.

At times video surveillance, which operates in or near our premises may capture images of you.

Other Parties
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.

Access
Subject to some exceptions that are set out in privacy law, you can gain access to the personal information that we hold about you.

Important exceptions include evaluative opinion material obtained confidentially in the course of our performing reference checks and access that would impact on the privacy rights of other people. We do refuse access if it would breach any confidentiality that attaches to that information or if it would interfere with the privacy rights of other people. In many cases, evaluative material contained in references that we obtain will be collected under obligations of confidentiality that we make and which the communicator of that information is entitled to expect will be observed.

If you wish to obtain access to your personal information you should contact our Partner, Amanda Mannix. You will need to be able to verify your identity.

We might impose a moderate charge in providing access. Our Partner would discuss these with you. You should also anticipate that it may take a little time to process your application for access as there may be a need to retrieve information from storage and review information in order to determine what information may be provided. We will generally respond to your request for access within 20 working days.

Electronic Transactions
This section explains how we handle personal information collected from our website and by other technology in the course of electronic transactions.

It is important that you understand that there are risks associated with use of the internet and you should take all appropriate steps to protect your personal information.
It is important that you:

- Know your rights: read our privacy policy, collection statement and consent to electronic transactions.
- Be careful what information you share on the Web.
- Use privacy tools on the site - control access to your search listing and profile.
- Make sure your anti-virus and data protection software is up-to-date.

Please contact our office by phone or mail if you have concerns about making contact via the internet.

Sometimes, we collect personal information that individuals choose to give us via online forms or by email, for example when individuals:

- ask to be on an email list such as a job notification list;
- register as a site user to access facilities on our site such as a job notification board;
- make a written online enquiry or email us through our website;
- submit a resume by email or through our website;

Browsing

When an individual looks at our website, our internet service provider makes a record of the visit and logs (in server logs) the following information for statistical purposes:

- the individual's server address
- the individual's top level domain name (for example .com, .gov, .org, .au, etc.)
- the pages the individual accessed and documents downloaded
- the previous site the individual visited and
- the type of browser being used.

We do not identify users or their browsing activities except, in the event of an investigation, where a law enforcement agency may exercise a warrant to inspect the internet service provider's server logs.

We do not accept responsibility for the privacy policy of any other site to which our site has a hyperlink, and it is advisable to look at the privacy policy of other sites before disclosing personal information.

Cloud Computing Services

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 or against third parties 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.

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 Privacy Principles. 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 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.

Social Networks and Web Searches
In order to assess your suitability for positions and to assist you to find work, we will need to collect, use and disclose personal information about you. It has become common practice in some places for employment service providers to conduct background checking via social network media sites frequented by candidates.

We will not conduct background checking via social network media sites other than those that you identify and authorise us to check. However, we do conduct internet searches using search engines and entering your name and relevant identifying details.

Uploading photographs
We will not upload photographs of any individuals who have not given consent to the display of their photograph.

Emails
Our technology systems log emails received and sent and may include voting, and read and receipt notifications to enable tracking.

When your email address is received by us because you send us a message, the email address will only be used or disclosed for the purpose for which you have provided it and it will not be added to a mailing list or used or disclosed for any other purpose without your consent other than as may be permitted or required by law.

Call and message logs
Our telephone technology (systems and mobile phones) logs telephone calls and messages received and sent and enables call number display.

When your call number is received by us because you phone us or send us a message, the number will only be used or disclosed for the purpose for which you have provided it and it will not be added to a phone list or used or disclosed for any other purpose without your consent other than as may be permitted or required by law.

Teleconferences and Video conferences
Teleconferences and video conferences may be recorded with your consent. In cases where it is proposed that they be recorded, we will tell you first the purpose for which they are to be used and retained.

Database
We use recruiting software and databases to log and record recruitment operations.

Paperless Office
Recognising the environmental advantages and efficiencies it provides, we operate a wholly/partially paperless office as a result of which your paper based communications with us may be digitised and retained in digital format, the paper based communications may be culled.

It is therefore important that, except where specifically requested, you do not send us originals of any paper based document and that you retain copies for your own records.

Where we do request original paper based documents, we will return them to you once they are no longer required by us for the purpose for which they may be used or disclosed.

Future Changes
This policy may change over time considering changes to privacy laws, technology and business practice. If you use our website regularly it is important that you check this policy regularly to ensure that you are aware of the extent of any consent, authorisation or permission you might give.

Inquiries and Complaints
You can make further inquiries or complaints about our privacy policies to our Partner, Amanda Mannix whose contact details are +61 7 3012 6640.

You can also make complaints to the Privacy Authorities in your national, state or territory jurisdiction.