# Privacy Policy

**This Privacy Policy outlines how Newcastle Rescue & Consultancy Pty Ltd manages personal information in accordance with the Privacy Act 1988 (Cth) and the Australian Privacy Principles (APPs). This policy is available upon request and is published on our website. Responsibility for privacy compliance rests with senior management, supported by staff training and internal procedures.**

Newcastle Rescue & Consultancy Pty Ltd respects the importance of securing any form of personal information which is collected from the participant/s and/or other Stakeholders. Newcastle Rescue & Consultancy Pty Ltd promotes and conducts the following policy in accordance with the Privacy Act 1988, as amended from time to time, and the Australian Privacy Principles (APP's) contained within the Privacy Act.

## Collection of Personal Information

Personal information may be collected directly from you, or on your behalf from a representative you have authorised.

We may also obtain personal information collected by Government agencies, third parties, or from publicly available sources.

We will only collect information that is:

- For lawful purposes that is reasonably necessary or;
- directly related to one or more of our functions or activities or;
- where otherwise authorised by law.

Under the Australian Privacy Principles, we are required to notify you of the purposes for which we collect information, whether the information collection is required or authorised by law, and any person or organisation/agency to whom we usually disclose the information. This is notified by privacy notices contained in our paper forms and electronic enrolment systems.

## Types of Personal Information Which May Be Collected and Held by Us

- Your name, address, contact details.
- Personal information such as marital status, age, gender, occupation, indigenous status.
- Emergency contact person name, relationship to you and contact details.
- Identity details such as your date of birth, country/town of birth, visa details, passport details, drivers Licence or other forms of identification required to satisfactorily confirm your identity.
- Information about your background such as educational background, year finished school, qualifications, English proficiency or other languages you speak.
- Your banking/credit card details in order to receive/make payments from/to you.
- Your Unique Student identifier (USI) number.
- Your employment status, employer name, job title, commencement date and contact person.
- Information about any disabilities, impairments or health conditions you may have.
- Your reason for undertaking the training course.
- Tax file number to make payments of salaries and wages to eligible employees.

**Collection of Sensitive Information**

In carrying out our functions and activities we may collect information about you which is sensitive.

'Sensitive information" is personal information about you that is of a sensitive nature such as: health, genetics, disability, racial or ethnic origin, religious, political beliefs, sexuality, criminal record.

We may only collect information from you that is sensitive:

- Where you provide your consent; or
- Where required by law; or
- Where a situation exists that presents a serious threat to life, health or safety.

We also collect sensitive information for the purpose of human resource management functions where lawful and reasonably necessary.

**How We Collect Personal Information**

We use paper forms and electronic means to collect your personal information. By signing paper documents or agreeing to the terms and conditions and disclaimers for electronic documents you are consenting to the collection of any personal information you provide to us.

We may also collect personal information from you if you:

- Communicate with us by telephone, mail, email, fax or SMS.
- Attend a face-to-face meeting or event conducted by us.
- Use our website.
- Interact with us on social media.

In certain circumstances, we may collect and receive personal information about you from third parties including government agencies where lawful and permitted.

**Remaining Anonymous or Using a Pseudonym**

Should any participant or Stakeholder choose to remain anonymous or use a pseudonym the individual has the right when it is lawful and practicable to do so.

**Use and Disclosure of Personal Information**

We use and disclose personal information only for the primary purpose for which it was collected, or for a related secondary purpose that you would reasonably expect.

Personal information may be disclosed to:

- Government agencies as required or authorised by law;
- Training regulators and data collection authorities;
- Contracted service providers who assist us in delivering training, assessments, administration, IT systems or compliance functions;
- Professional advisers such as accountants, auditors or legal advisers (where required).

We do not sell personal information or use it for unrelated marketing purposes without your consent.

**Purposes for Which Information is Collected, Held, Used or Disclosed**

We collect personal information for a variety of different purposes relating to our functions and activities including:

- Performing human resource management functions in relation to our staff and contractors;
- Performing legislative and administrative functions;
- Policy development, research and evaluation;
- Complaints handling
- Contract management
- Management of correspondence

**Storage and Data Security**

We hold personal information in a range of paper-based and electronic records.

Storage of personal information (and disposal of information when no longer required) is managed in accordance with the requirements of:

- Standards for RTOs 2015
- Student Identifiers Act 2014
- Privacy Act 1988
- VET Data Policy 2018
- Data provision requirements 2012
- National Vocational Education and Training Regulator Act 2011
- VET Quality Framework

Electronic records containing personal information are protected in storage within our Student Management System (Wisenet) and SharePoint and are accessible only to authorised staff with password-protected access.

Paper records containing personal information are stored and protected in locked filing cabinet in a locked room at our office.

**Disposal of Personal Information**

Disposal occurs:

1. Six months after training course has been completed or certificate has been issued whichever is the latter (for paper files, by secure document disposal) unless a longer retention period is required by law.
2. Once enrolment is completed and certificate has been issued, enrolment is disabled within the Student Management System while records required for regulatory retention remain securely stored. Information contained in the student management system is only accessible to authorised employees.
3. In accordance with the Student Identifiers Act 2014, Information collected solely for the purpose of making a USI application is destroyed immediately after the application is made.

**Data Breaches and Incident Response**

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

In the event of a suspected or actual data breach, we will assess the incident in accordance with the Notifiable Data Breaches scheme. Where a breach is likely to result in serious harm, we will notify affected individuals and the Office of the Australian Information Commissioner (OAIC)
as required by law.

**Accessing and Correcting Your Personal Information**

You have a right to access the personal information we hold about you. You also have the right to request corrections of any personal information we hold if you think it is inaccurate, out of date, incomplete, irrelevant or misleading.

To access or seek correction of personal information we hold about you please contact us. If you request access to your information for correction purposes, we must respond to you within 30 calendar days.

The Privacy Act requires us to give you access to correct your personal information however it does set out circumstances in which we may refuse you access or decline to correct your personal information. If we refuse to give you access or decline to correct your personal information we will provide you with a written notice which among other things gives our reasons for refusing your request.

It is possible to access documents held by us under the freedom of information act 1982.

If you are unsatisfied with our response, you may make a complaint, either directly to us or you may contact:

The office of the Australian Information commissioner at enquiries@oaic.gov.au or phone 1300 363 992.

**Overseas Disclosure**

Some of our electronic systems, service providers or data storage solutions may involve the handling or storage of personal information outside Australia.

Where personal information is disclosed overseas, we take reasonable steps to ensure the overseas recipient complies with the Australian Privacy Principles or equivalent privacy protections, unless an exception under the Privacy Act applies or you have provided informed consent.

**Government-Related Identifiers**

Government-related identifiers (such as Tax File Numbers, passport details, driver licence numbers and USI details) are collected and used only where authorised by law. We do not adopt government identifiers as our own internal identifiers and handle them in accordance with the Privacy Act.

**Direct Marketing**

We do not use personal information for direct marketing unless permitted by law or with your consent. You may opt out of any direct marketing communications at any time.

**Automated Decision-Making**

We do not currently use automated decision-making systems that produce legal or similarly significant effects for individuals. If this changes, this policy will be updated and affected individuals notified.

**Complaints**

If you believe we may have breached your privacy and wish to make a complaint, please contact us on 1300 356 686 or via email enquiries@newcastlerescue.com.au. We prefer, to ensure we fully understand the nature of your complaint, that you make your complaint in writing. It may be difficult for us to properly handle your complaint if you provide insufficient detail.

Your compliant can be made anonymously however, we may not be unable to provide a response to you. All complaints are taken seriously and investigated appropriately. No complainant will be victimised or treated negatively if they make a compliant.

If you are unhappy with the way we handle your complaint you may contact the Office of Australian Information Commissioner to refer your compliant for further action.

Phone: 1300 363 992

Email: enquiries@oaic.gov.au

All employees of NRC who have access to your personal information are trained in the content of this policy and are required to follow documented data protection procedures.