Privacy Policy

Policy statement	To ensure Relationships Australia Victoria (RAV) fulfils its obligation to maintain the privacy of clients, students, employees, contractors, RAV takes its privacy obligations very seriously. RAV expects all staff, managers, students, contractors, to respect the confidentiality of all personal information and to use that information in a sensitive manner and only for the purpose for which it was collected.
Scope	All RAV Staff, clients, students and contractors
Content Areas	1. Purpose 2. Consent 3. Management of personal information 4. Using a pseudonym 5. Retention of information 6. Access to personal information 7. Correction of information 8. Complaints 9. Disclosure to overseas recipients 10. Taking photos, videos and other images 11. Image of children 12. Public events 13. Copyright 14. RAV Training department – student information 15. Evidence of Compliance 16. Responsibility and Accountability
Definitions	1.1. **Personal information** – Under the *Privacy Act (1988)* and in this policy, personal information means "information or an opinion about an identified individual, or an individual who is reasonably identifiable: i. Whether the information or opinion is true or not; and ii. Whether the information or opinion is recorded in a material form or not" 1.2. **The Australian Privacy Principles** *(Privacy Act (1988))* outline how not-for-profit organisations must handle, use and manage personal information.

1. Purpose

RAV collects and uses personal information for the purpose of carrying out its functions and activities, including (but not limited to) assessment, service provision, fulfilling duty-of-care responsibilities, correspondence, invoicing and promotional material, including photos. This information ranges from name and contact details to a client's relevant personal history related to the service to be provided, to student information to staff personal information and promotional images.

2. Consent

2.1 The four key elements of consent are:
- The individual is adequately informed before giving consent
- The individual gives consent voluntarily
- The consent is current and specific, and
- The individual has the capacity to understand and communicate their consent.

2.2 Implied consent arises where consent may reasonably be inferred in the circumstances from the conduct of the individual and RAV.

2.3 As general principle, an individual under the age of 18 has capacity to consent when they have sufficient understanding and maturity to understand what is being proposed. In some circumstances, it may be appropriate for a parent or guardian to consent on behalf of a young person, for example, if the child is young or lacks the maturity or understanding to do so themselves.

2.4 If it is not practicable or reasonable for RAV to assess the capacity of individuals under the age of 18 on a case-by-case basis, RAV may presume that an individual **aged 15** or over has capacity to consent, unless there is something to suggest otherwise. An individual aged under 15 is presumed not to have capacity to consent.

3. Management of personal information

3.1 RAV holds personal information in both 'hard copy' files in secure filing cabinets and electronically via its secure databases.

3.2 If there in any doubt about the proposed collection, use or disclosure of an individual's information, all staff must consult with their Manager. This obligation applies to all personal information i.e. information about an identified individual (whether or not the person is yet registered as a client or student or employed as a staff).

3.3 RAV will usually collect personal information about an individual only from the individual unless RAV is authorised by law or Court/Tribunal order to collect it from someone else.

3.4 RAV will only collect information without the consent of the individual when:
- a) The information is reasonably necessary for one or more of its functions or activities; or
- b) The collect is required or authorised by Australian law or a Court/Tribunal order; or
- c) It is reasonable or impracticable to collect it from the individual, or with the consent of the individual
- d) A "permitted general situation" or a "permitted health situation" exists. (see 3.6 and 3.7 below).

3.5 Generally speaking, employees, interns and students, or contractors of RAV must not disclose an individual's personal information to anyone outside RAV, including government departments, unless the individual has consented to that disclosure. However, there are some exceptions; see below.

3.6 Personal information may be disclosed if "a permitted general situation" exists;
- 3.6.1 to comply with the Family Law Act (FLA) obligations to report child abuse or risk of such abuse to a child welfare authority (in Victoria, the Department of Health and Human Services);
- 3.6.2 if there is physical or psychological risk to a child, or where there is a serious and imminent risk to the life or health of any person;
- 3.6.3 to report a crime of violence or prevent the likely commission of a crime of violence;

3.6.4 if there is a need to prevent or lessen a serious and imminent threat to the property of a person or prevent or lessen likely damage to property;
3.6.5 to assist an independent children's lawyer to properly represent a child's interests in Court;
3.6.6 if RAV receives a subpoena or witness summons for information about an admission by an adult, or disclosure by a child, of child abuse or risk of such abuse;
3.6.7 if RAV receives a subpoena or witness summons for information in legal proceedings unrelated to family law e.g. criminal proceedings;
3.6.8 if a Court/Tribunal orders RAV to disclose.

3.7 A "permitted health situation" applies when an organisation is collecting health information about an individual, if the information is necessary to provide a health service to the individual, and either:
3.7.1 the collection is required or authorised by or under an Australian law (other than the Privacy Act), or
3.7.2 the information is collected in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation (s 16B(1)).

3.8 When an individual is engaged in different programs within RAV, relevant personal information may be shared between RAV's practitioners when seen to be in the client/s best interests and when necessary to permit greater understanding of the client/s situation, in order to benefit service delivery within each program. An individual may request that his/her information not be shared between programs and no information may then be shared. (exception: "permitted general situation" see 3.6 above).

3.9 In a variety of situations, RAV collects, or is invited to accept, unsolicited personal information about an individual from someone other than the individual e.g. information provided by another person at intake/assessment (e.g. former or current partner), oral referrals by telephone (e.g. from DHHS), Family Reports.

3.10 In most cases, it is likely that RAV would have collected the information (because it is reasonably necessary), and it is reasonable to hold the information.

3.11 If the information is not reasonably necessary for its functions or activities, RAV must, as soon as practicable, destroy or de-identify any such information.

3.12 RAV must also take such steps as are reasonable in the circumstances to notify the individual of the collection and the circumstances of that collection. It is a matter of clinical judgement as to whether it is reasonable to notify the individual accordingly.

3.13 Employees, interns and students of RAV must take such steps as are reasonable in the circumstances to protect personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure. All staff and students on placement, have a responsibility to ensure that clients' personal information is kept secure, and must ensure that files and computers are not left unattended in any area accessible by the public. This responsibility applies also to any necessary transportation of personal information outside the centre; for more detail, see Case Notes and File Management Procedure.

4. Using a pseudonym

4.1 Under the amending Act, an individual has the option of not identifying himself/herself, or of using a pseudonym, but this does not apply if:
a) RAV is required or authorized by law or a Court/Tribunal order to deal with individuals who have identified themselves (i.e. mandated clients);
b) it is impracticable for RAV to deal with individuals who wish to remain anonymous or use a pseudonym.

In special circumstances RAV will agree to a request by an individual to use a pseudonym, except in the circumstances outlined at 3.6 of this policy. An attempt should first be made to establish the identity of the individual and allay anxiety about the security of that information. However, where a person still prefers to provide a pseudonym that will be accepted. Contact details (address and telephone number) will still be required.

5. Retention of information

5.1 If personal information is no longer needed for any purpose for which it may be used or disclosed, and RAV is not required by law to retain the information, RAV will take reasonable steps to destroy or de-identify the information. Under the Health Records Act 2001 (Vic), unless deletion is permitted or required under another law (e.g. Privacy Act 1988 (Commonwealth), RAV is required to retain "health information" for a period of seven (7) years, and records relating to children until the child turns 25 years of age. Because of the uncertainty about determining when Family Dispute Resolution (FDR) information is no longer needed, and for administrative convenience, RAV retains FDR information for the same periods of time. See also Case Notes and File Management Policy, Control of records Policy. In the case of 'pre-case records' (i.e. file notes or other records of initial telephone conversations or other contact with an individual, before the person becomes a client), these records will be kept securely for a period of two (2) months and then destroyed, unless the individual becomes a client within that time, in which case the notes must be placed on the client's file.

5.2 All practitioners and managers (and administrators when necessary) must keep a comprehensive record of any matter or decision that relates to the use or disclosure of an individual's personal information, or to contact with the individual about their information, including discussions/correspondence/emails and telephone calls from and to the individual.

6. Access to personal information

6.1 All requests by an individual or client for access to personal information must be referred to the manager of the centre that has provided the service delivery. Such requests may be made orally but must be confirmed in writing. The consent of that manager is required before any personal information can be released.

6.2 Subject to 3.6, if RAV holds personal information about an individual, RAV must, upon request by the individual, give the individual access to the information.

a. RAV must respond within 30 days after the request is made;
b. RAV must give access in the manner requested by the individual, if it is reasonable and practicable to do so. If RAV refuses to do this, it must take such steps (if any) as are reasonable in the circumstances to give access in a way that meets the needs of RAV and the individual.
c. RAV can refuse both access and correction requests in particular situations, however if this occurs, a statement of reasons is to be provided to the client.

6.3 A client is not entitled to access any information/file notes relating to joint or group service delivery. It is considered that giving access in such circumstances would have an unreasonable impact on the privacy of other individuals.

6.4 A client may access joint or group session information if he/she obtains the prior written consent of the other clients who attended the joint or group sessions.

6.5 RAV is not required to give the individual access to the extent that:

6.5.1 it believes that giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety; or

6.5.2 giving access would have an unreasonable impact on the privacy of other individuals; or
6.5.3 the request is frivolous or vexatious; or
6.5.4 giving access would be unlawful; or
6.5.5 denying access is required or authorized under Australian law or a Court/Tribunal order.

6.6 If access is refused, or access in the manner requested by the individual is refused, the individual must be advised in writing of the reasons for refusal (except to the extent that it would be unreasonable to do so), and of the mechanism to complain about the refusal.

7. Correction of information

7.1 RAV must take all reasonable steps to ensure that an individual's personal information collected, used or disclosed is accurate, up-to-date, complete and relevant. If RAV becomes aware that an individual's personal information is inaccurate, out-of date, incomplete, irrelevant or misleading, or an individual requests that RAV correct his/her information for these reasons, RAV must take such steps as are reasonable in the circumstances to correct the information.

7.2 RAV will note the changes requested within 30 days after the request is made. Under no circumstances can case or file notes be changed. Any requested changes must be noted on an additional Cast Note Template and a summary added to the Case File Summary Form, dated and signed.

8. Complaints

8.1 If a person wishes to make a complaint about an alleged breach of the APPs, he/she should first complain, either orally or in writing, to the manager of the centre that has provided the service delivery. If the complaint is not resolved, the person should be directed to make the complaint in writing to the RAV Complaints' Officer, whose role it is to review, investigate and respond to the complaint. If still unresolved, the complaint will be referred to RAV's Chief Executive Officer for final attempted resolution within RAV. If the complaint remains unresolved, the person may complain to the Office of the Australian Information Commissioner (OAIC). This complaint must be made in writing and may be made at any time after 30 days from the date of making the original complaint to RAV. All responses within RAV should be as prompt as possible, bearing in mind the person's right to complain to the OAIC.

9. Disclosure to overseas recipients

Under the amending Act, RAV's Privacy Policy must advise whether it is likely to disclose personal information to overseas recipients. Since RAV's activities are confined to Australia, it is rare that RAV needs to disclose personal information to an overseas recipient. Subject to the exceptions in 3.6, RAV will not disclose any personal information to an overseas recipient without the client's clear consent.

10. Taking photos, videos and other images

10.1 The Privacy Act protects personal information that is held, or collected for inclusion, in a 'record'. A 'record' is defined to include a photograph or other pictorial representation of a person. If an individual's identity is apparent, or can reasonably be ascertained, from a photograph or other image, then the collection, use and disclosure of that image is covered by the Privacy Act. This extends to video images as well as still photographs.

10.2 If a person is identifiable in a photograph, the ideal approach in all cases is to obtain the informed and voluntary consent of the people in the pictures. RAV will, as often as possible, give notice to people attending an event that photos will be taken for specific purposes.
10.3 Consent will be obtained by completing the "Consent to collect and use photographs and images of people" or associated specific form.
10.4 If a person expressly requests that their image is not to be published, RAV will respect that person's right to privacy.
10.5 RAV will retain and use the images for no longer then five (5) years after the date on the consent form.
10.6 RAV consent to their imagery being used for RAV purposes only, as outlined in the compliance agreement.

11. Images of children

11.1 Parental consent must be obtained for children up to the age of 18.
11.2 If parents disagree over consent, then it is deemed that consent is NOT given.
11.3 It parents agree, but the child does not, then it is deemed that consent is NOT given
11.4 A person between the ages of 15 to 18 years can provide consent if they have the intellectual capability and maturity to understand the consequences of consenting.
11.5 As a general principle, an individual under the age of 18 has capacity to consent when they have sufficient understanding and maturity to understand what is being proposed. In some circumstances, it may be appropriate for a parent or guardian to consent on behalf of a young person, for example, if the child is young or lacks the maturity or understanding to do so themselves.
11.6 If it is not practicable or reasonable for RAV to assess the capacity of individuals under the age of 18 on a case-by-case basis, RAV may presume that an individual **aged 15** or over has capacity to consent, unless there is something to suggest otherwise. An individual aged under 15 is presumed not to have capacity to consent.

12. Public events

Representatives of RAV are often tasked with taking photos and videos at public events, at which RAV has a presence (presentation, stall, public facing work).

12.1 Prior to the event RAV representatives must answer the following:
- Would people attending the event expect photographs to be taken?
- Would people in the photograph consider themselves to be in a public place and not have reasonable expectation of privacy?
- Do you think it's unlikely that anyone would object to the photograph being taken?

If the answer to any of these questions is 'no', then it is not appropriate to take photos at the event.
If the answer to any of these questions is 'yes', then photos can be taken to provided that RAV:

12.2 Ensures that promotional flyers for the event (if prepared by RAV) contain the following statement: *Photos and videos will be taken at this event, if you do not want to be included in photos or videos taken at this event please let the organisers know.*

12.3 Makes it clear through announcement (if practicable) and the placement of notices at the event, that photos may be taken, and if members of the public have any concerns, to talk to a RAV staff member.
12.4 Places notices at the event detailing how to contact the organisation to advise on any privacy concerns
12.5 Checks with the hosting venue for their rules on taking photos and videos, and ensures that RAV complies with these rules.
12.6 Collects completed consent forms from people whom feature in photos and videos intended for use by the organisation in advertising or promotional material, where the number of people appearing in the photo or video is five or less. Note: where photos or videos of groups of more than five people are taken, completed consent forms are not required, provided that points 4.2 to 4.5 have been undertaken.
12.7 Maintains current records of photos/videos and associated/linked consent forms in formal registers at each centre.

13. Copyright

13.1 Photos taken under a contract may not be used other than the purpose for which they were intended without the permission of the photographer. This means that the subject of a photo does not have copyright on the photo simply because they are the subject.

14. RAV's Training Department – student information

Collection of personal information

14.1 RAV is required to collect personal information from students in order to process enrolments and obtain the information required to provide suitable training and assessment services. Where applicable, information may also be required to comply with ASQA standards as specified by government regulators.
14.2 Information collected includes general personal details, and may include details of any disability or health issue that may affect the student's ability to undertake training and/or assessment activities.
14.3 RAV will only collect personal information that is required for the purposes of education, or in meeting government reporting requirements.
14.4 RAV collects all personal information in writing on an enrolment form, directly from the person whom the information is about.
14.5 RAV uses personal information of its students for the purposes of meeting VET requirements for the awarding of national qualifications, and to comply with reporting requirements where relevant, as specified by government regulators.
14.6 Personal information collected through the enrolment form or through other means will be passed on to government regulators as per legal data collection requirements. This personal information may also be accessed for the purposes of an audit by the ASQA.
14.7 Student information will be kept electronically for 30 years to be able to reissue a qualification or statement of attainment. If RAV ceases being an RTO, the information will be provided to ASQA in digital form.
14.8 Unique Student Identifier (USI) From 1 January 2015, students undertaking nationally accredited training with RAV (i.e. enrolling into VET courses) will need to set up a Unique Student Identifier (USI)

15. Evidence of compliance

- All client information gathered by RAV is relevant to the case and created, managed, archived and destroyed in accordance with the Client Case File Management Procedure.

- Any changes to client cases and/or files is recorded.
- Regular internal case file audits will be undertaken, as determined by the RAV Quality Management Committee, to ensure continued compliance with RAV organisational, contractual and legal obligations.

16. Responsibility and accountability

- Managers are responsible for ensuring that staff members are informed about this policy and for ensuring compliance.
- All staff members are responsible for reading nad complying with this procedure.

Regulatory References	1. The *Privacy Act* (1988) 2. Australian Privacy Principles Guidelines. Australian Information Commissioner Feb 2015 3. Standards for registered Training Organisations 2015 4. Australian Skills Quality Authority (ASQA)
Organisational References	1. Data Management Policy & Procedure 2. ICT Security Policy (under development) 3. Client File Management Procedure 4. Research Policy 5. Values Policy 6. Code of Ethics Policy 7. Access & Equity Policy
Consultation Group	QMC
Approver	Chief Executive Officer
Custodian	Senior Manager – Practice Development