

## POL 4.2 Privacy

### Scope

This policy conforms to the [Privacy Act 1988](#) (Cth) (Privacy Act) (including the [Australian Privacy Principles](#) contained in Schedule 1), of the [Health Records Act 2001](#) (Vic), and the [Privacy and Data Protection Act 2014](#) (Vic) (including the [Victorian Information Privacy Principles](#) contained in Schedule 1), which govern the collection, use and storage of Personal Information.

Housing Justice is also required to comply with the Family Violence Information Sharing Scheme as described in Part 5A of the [Family Violence Protection Act 2008](#) (Vic) and the [Family Violence Multi-agency Risk Assessment and Management \(MARAM\) Framework](#). The CLC is not an information sharing entity.

This policy does not include the obligations of solicitors to legal professional privilege, a duty of confidentiality and the provisions of the *Legal Profession Act 2004* and the *Professional Conduct and Practice Rules 2005*. These obligations are covered in specific detail in the NACLC Risk Management Guide and form part of the Community Legal Services Program (CLSP) funding agreements.

ARC Justice is obligated under federal privacy laws to comply with the relevant Australian Privacy principles (APPs).

### Responsibilities

<b>Compliance:</b> All staff, students and board members	<b>Review:</b> Management Team	<b>Approval:</b> Chief Executive Officer
----------------------------------------------------------	--------------------------------	------------------------------------------

### Definitions

**Client Records:** any information about a client whether in electronic or paper form.

**Consent:** is an approval provided by a person, which can be given expressly (either orally or in writing) or impliedly (inferred in the circumstances). The individual must have the capacity to understand and communicate their consent. Consent must be informed, given freely, specific, and current.

**Data Breach:** occurs when Personal Information held by an organisation is subject to unauthorised access or disclosure or is lost. A data breach can harm an individual/s whose personal information is affected.

**Information Barrier:** An information barrier is an arrangement designed by organisations to prevent the flow of information from one department to the other. It prevents communication between separate departments that may lead to a conflict of interest.

**Personal Information:** means information or an opinion about an identified individual, or an individual who is identifiable: whether the information or opinion is true or not; and whether the information or opinion is recorded in a material form or not. 'for example, a person's Name, address, contact details, date of birth, gender, sexuality and race.

**Privacy:** includes an individual's right to be free from interference and intrusion, to associate freely with others, and to be able to control who can see or use their Personal Information.

**Privacy Officer:** An organisation may appoint a person ('privacy officer') to be responsible for developing, implementing and updating its privacy policy, and to be the first point of contact for privacy issues or complaints.

**Privacy Statement:** is a statement that explains in simple language how ARC Justice handles Personal Information which is accessible on ARC Justice website or provided to clients during their initial consultation.

**Sensitive Information:** is information or an opinion about a person's racial or ethnic origin, political opinions, religious beliefs, membership sexual orientation or practice.

**Health Information:** is information or opinions about a person's physical or mental health, disability, health preferences, use of health services or bodily donations

**Serious harm:** includes identify theft, financial loss through fraud may include serious physical, psychological, emotional, financial, or reputational harm to an individual.

**Staff records:** Any electronic or paper documents that include individual staff's personal information.

## Policy Statement

### 1. Our commitment to Privacy

ARC Justice is committed to protecting and upholding the Privacy of our clients, staff, volunteers, board members and representatives of other agencies. In particular ARC Justice will ensure we maintain Privacy in the way we collect, store and use Personal Information.

Clients will be provided with information regarding what Personal Information is being collected, how their Privacy will be protected and their rights in relation to their Personal Information.

A summary of the privacy policy is available on the website and the full policy will be provided free of charge upon request. When requested by clients, the organisation will provide information regarding the collection, use and disclosure of their Personal Information.

ARC Justice will respond to inquiries or complaints from individuals about the organisation's compliance with the Australian Privacy Principles.

### 2. Australian Privacy Principles (APPs)

The APPs are legally binding principles which are the cornerstone of the privacy protection framework in the Privacy Act. - The APPs set out standards, rights and obligations in relation to handling, holding, accessing and correcting personal information.

The APPs consist of:

- APP 1** Open and transparent management of personal information
- APP 2** Anonymity and Pseudonymity
- App 3** Collection of personal information
- App 4** Dealing with Unsolicited personal Information
- App 5** Notification of the collection of personal information
- APP 6** Use and Disclosure of Personal Information
- APP 7** Direct Marketing
- APP 8** Cross Boarder disclosure of personal information
- APP 9** Adoption, use or disclosure of government related identifiers
- APP 10** Quality of Personal information
- APP 11** Security of personal information
- APP 12** Access to personal information
- APP 13** Correction of personal information.

ARC Justice is responsible in all circumstances to implement practices, policies, procedures and activities that comply with the Australian Privacy Principles. All APPs have been considered and applied to the policy statements in this document.

### **3. Who is responsible for managing Privacy?**

All staff are responsible for the management of Personal Information to which they have access and will comply with this policy and any relevant procedures. Staff are provided with this policy as part of employment and may in addition be asked to sign a more specific confidentiality agreement if their role requires.

The People and Shared Services Manager has the role of the Privacy Officer to support and coordinate any known or possible Privacy and Data Breaches. If any staff have any questions about the processes in place to maintain and manage privacy, please contact the **Privacy Officer** via [privacy@arcjustice.org.au](mailto:privacy@arcjustice.org.au)

### **4. Collection**

ARC Justice will only collect, use and store Personal Information (identifiable) that is necessary for the functioning of the organisation and its activities.

ARC Justice will ensure the collection of client Personal Information optimises privacy (e.g., using private interview rooms) and accuracy (e.g. collecting or confirming information with the client).

Steps will be taken to ensure Personal Information collected, including Sensitive Information if applicable, is relevant, up-to-date and complete and not collected in an unreasonably intrusive way.

Staff will take reasonable steps to protect all Personal Information from misuse and loss, and from unauthorised access, modification or disclosure.

When collecting necessary Sensitive and Health Information, ARC Justice will get the persons consent, unless an exception applies.

Sensitive Information regarding a client's health and/or medical treatment is only collected, recorded on file, disclosed, communicated or transferred to someone outside of Victoria (in line with the *Health Records Act 2001* (Vic)) if it directly relates to their case with ARC Justice and the client has provided their Consent.

APP requires that individuals be made aware of their opportunity to deal anonymously or by pseudonym where applicable. There may be a limited number of circumstances, such as when providing general information, that a client can request to remain anonymous or use a pseudonym. In general, however it is impracticable to provide a legal or housing advocacy service to individuals who have not identified themselves.

ARC Justice does not receive unsolicited information. If unsolicited personal information is received (for example incorrectly from another organisation) this will be destroyed, and the source informed.

### **5. Information provided to clients and consent**

Clients will be made aware of why Personal Information is being collected and specific Consent will be sought to use of Sensitive Information

Clients will be made aware of and given the opportunity to consent to:

- who is collecting their information, including contact details.

- what type of Personal Information is being collected, including whether Sensitive or Health Information is being collected.
- why their information is being collected.
- what their information will be used for (including potential secondary uses).
- how the person can get access to their Personal Information.
- who else will have access to their Personal and Sensitive Information?
- what the main consequences, if any, are for the person if they do not provide the information.
- whether their de-identified Personal Information (and if applicable their Sensitive Information) will be shared with funders and used for statistical or secondary uses such as research; and
- how long their information will be stored and the means of storage (i.e. secure electronic database, Cloud storage, locked filing system).

Consent will be recorded in writing; Consent can be revoked by the Client at any time by advising a member of staff. Client's may also revoke their consent by contacting [privacy@arcjustice.org.au](mailto:privacy@arcjustice.org.au).

Clients must be informed of or given access to their rights and responsibilities regarding their Personal Information, for example by being provided the Privacy Statement. This Privacy Statement lists the potential secondary uses of their Personal Information (including Sensitive Information if applicable) to ensure that their collected Personal Information can be used for secondary purposes such as for research, auditing and systematic advocacy.

## **5. Use and Disclosure of Personal Information**

ARC Justice will only use Personal Information for the primary purpose for which it was collected, or a permitted secondary purpose unless an exception under state or federal law applies, e.g. Personal Information can be disclosed to protect an individual from Serious Harm.

Staff will consider if it is appropriate to identify their service (e.g., Community Legal Centre (CLC) or HJ (Housing Justice) or leave a message with a third party, unless there is prior client Consent.

Staff will also consider if it is safe and appropriate to send clients letters to the address provided.

Staff will not release information about a deceased client unless it is in accordance with relevant legislation.

Clients are required to provide Consent to the use or disclosure of their Personal Information for any secondary purpose other than the primary purpose, unless:

- the secondary purpose is related to the primary purpose of collection and, if the Personal Information is Sensitive Information, directly related to the primary purpose of collection, the client would reasonably expect ARC Justice to use or disclose the information for the secondary purpose; or
- the use or disclosure is required, authorised by or under law; or
- the use or disclosure is necessary for research, or the compilation or analysis of statistics, in the public interest, other than for publication in a form that identifies any particular individual; or
- ARC Justice believes that the use or disclosure is necessary to lessen or prevent a serious threat to an individual's life, health, safety or welfare, or to the public's health, safety or welfare; or
- ARC Justice believes that the use or disclosure is reasonably necessary for one or more law enforcement related activities by law enforcement agencies for example in the prevention,

- detection, investigation, prosecution or punishment of criminal offences or the protection of public revenue; or
- Australian Security Intelligence Organisation or the Australian Secret Intelligence Service has requested the ARC Justice to disclose the Personal Information.

If it is necessary for the purpose of law enforcement related activities by law enforcement agencies to use or disclose Personal Information without a client's Consent, a written note of the use or disclosure must be recorded.

ARC Justice does not use or disclose client information for direct marketing to promote goods and services or fundraising. ARC Justice will not adopt a government related identifier and would only disclose this information with consent from a client as other personal information is handled.

## **6. Storage, security and destruction of personal information**

All Client Records will be kept securely, updated, archived, and destroy or de-identified according to legislation and the service specific client records policies.

ARC Justice will take all reasonable measures to ensure Personal Information is stored safely to protect it from misuse, loss, unauthorised access, modification or disclosure, including electronic and physical security measures (with the support of the ICT (Information and Communication Technology) contractor). Personal information will be stored in servers located in Australia as per requirements of funders, state and federal government legislation and in line with the privacy principles

ARC Justice will store Personal Information in different ways, including in paper and in electronic form and on client management systems. Electronic files, records and data concerning clients are kept on the secure Microsoft Teams platform specific to the relevant program that is protected from unauthorised access from outside ARC Justice. Strong passwords are required to access any computer on the ARC Justice network and two factor authentication is used.

Client Records will not be removed from the office unless necessary (for example to attend court, counsel's chambers, prison, mediation, health services or to a client interview).

Where Client Records are required to be removed from the office, a program specific client file movement register will be used. The current location of a file, the name of any person who removed it, the date of the removal and purpose/destination is to be recorded in the file movement register. Client Records that are taken out of the office must not be accessible to other people, the client's name and identifying details must be concealed, and the Client Records must be secured in a locked bag/cabinet, returned to the office, and stored securely as soon as possible. See POL 11.4 Client data and file management policy

Client Records or data will not be taken out on portable data storage devices (for example, USB flash drives or CDs etc) unless absolutely necessary and at a minimum password protected. Client Records or data stored on a laptop taken outside the CLC will also be password and security protected.

Personal Information regarding ARC Justice staff, board members, and volunteers and will be maintained and protected in accordance with privacy legislation and as per **PRO 8.13 Staff records**.

Client and staff records will be destroyed following the necessary period in line with privacy requirements. Special considerations apply to Commonwealth records, which can only be destroyed or altered in accordance with the Archives Act 1983 (Archives Act).

## 7. Access to Personal Information and correction

All clients have the right to request access their Personal Information except where it is expressly prohibited by law. Clients are informed of their rights to access their Personal Information and are informed of the process of how this can be carried out as per **PRO 4.2 Access to confidential information**.

ARC Justice will take reasonable steps to correct personal information to ensure that, having regard to the purpose for which it is held, it is accurate, up-to-date, complete, relevant, and not misleading.

## 8. Information Barrier

ARC Justice is required to ensure an Information Barrier is maintained between the CLC and other ARC Justice or partnership programs that may be located within the same site to meet confidentiality and legal Practice Professional Responsibilities. This is managed as per **PRO 4.4 Information barrier**. It is acknowledged that ARC Justice does not have their own clients and the requirements for an information barrier in legislation and **the NACLC Risk Management Guide** is premised on this understanding. Accordingly, priority is given to an Information Barrier between programs of ARC Justice that have clients, namely the CLC and Housing Justice.

## 9. Family Violence Information Sharing Scheme

The Family Violence Information Sharing Scheme (FVISS or the Scheme) has been created through the new Part 5A of the [Family Violence Protection Act 2008](#) (Vic) (FVPA). The Scheme authorises a select group of prescribed information sharing entities (ISEs) to share information between themselves for family violence risk assessment and risk management as per [the Guidelines](#).

Any Personal Information, or Sensitive Information (including health information) that is relevant to assessing and/or managing family violence risk can be shared between ISEs, provided:

- the Personal Information or Sensitive Information is not considered "Excluded Information" under the FVPA.
- sharing the Personal Information or Sensitive Information does not contravene another law; and applicable Consent requirements have been met.

Housing Justice is an ISE (information sharing entities) and will manage FVISS requirements as per **PRO 12.10 Managing family violence risks and requirements**.

As an ISE, Housing Justice may share information with the CLC or any other non-ISE organisation in certain prescribed circumstances. Any information sharing must occur under other applicable laws, such as existing privacy laws, as Part 5A does not apply to the CLC. Personal Information can be shared with Consent, or without Consent if an organisation believes it is necessary to lessen or prevent a serious threat to an individual's life, health, safety, or welfare.

It is important to note that the word 'imminent' has been removed from the wording of *Privacy and Data Protection Act 2014* (Vic) and the *Health Records Act 2001* (Vic). 'Serious' threats should consider what a reasonable person would regard as 'serious'. In making the assessment, the severity and likelihood of the threat should be considered, and other factors such as timing, nature of the harm and vulnerability (i.e. if the affected individual is a child) may also be considered. Any recipient of such information should be in a position to act on it<sup>1</sup> – so, it is most likely that any sharing of information regarding threats should be made to the police in the first instance.

---

<sup>1</sup> Guidelines to the Information Privacy Principles (2011) 64.

## The CLC is not an information sharing entity.

### 10. Publications and communication

Any information used for publications and communications will be used with Consent.

### 11. Data Breaches

ARC Justice will act appropriately and in a timely manner in the event of a suspected or confirmed Data Breach, to contain the possible resulting harm in accordance with the OAIC (Office of the Australian Information Commissioner) requirements. This may include informing the appropriate clients and agencies involved and where necessary reporting to funders and government bodies. Data Breaches will be managed as per **PRO 4.3 Privacy data breaches and Pro 4.2 Access to confidential information.**

Any staff misconduct that relates to a breach of privacy will be managed as per **PRO 8.11 Issues resolution and grievance management.**

The People and Shared Services Manager has the role of the Privacy Officer to support and coordinate any known or Data Breaches. Administrative support may be provided to the Privacy Officer by the Quality and Compliance Officer.

### 12. Monitoring and evaluation

The application of this policy will be monitored and evaluated as part of the Compliance, Accreditation, Risk and Safety (CARS) report. This may include periodic audits and performance measures.

## Related policies, procedures and documents

This policy should be read in conjunction with:
<b>Policies:</b> POL 11.4 Client Data and File Management POL 4.1 Regulatory compliance
<b>Procedures:</b> PRO 4.1 Maintaining regulatory compliance PRO 4.2 Access to confidential information. PRO 4.3 Privacy data breaches PRO 4.4 Information Barrier PRO 8.9 Staff records. PRO 8.11 Issues resolution and grievance management. PRO 11.4 Client Data and File Management PRO 12.10 Managing family violence risks and requirements. PRO 12.8 Client file management
Documents/ resources
<a href="#">Australian Privacy Principles</a> <a href="#">Victorian Information Privacy Principles</a> NACLC Risk Management Guide <a href="#">Multi-agency Risk Assessment and Management (MARAM) Framework</a> <a href="#">Australian Cyber Security Services: Essential Eight</a>

[ACSC Homepage | Cyber.gov.au](#)  
[Privacy and information security guideline for funded agency staff-NFP Privacy Guide](#)

## Review and Revision history

This Policy will be reviewed at a minimum on a three yearly basis.

Date	Document History	Person
Oct 2012	Created in new format	Mim Dineen
Dec 2015	Reviewed	Management Team
Jan 2019	Adjusted to new format and reviewed	Isabelle Manning and CARS Committee
Mar 2019	Minor adjustment to refer to Policy Officer	Mim Dineen
May 2019	Minor adjustment to add MARAM Framework links	Mim Dineen
May 2020	Minor adjustment to align definition of confidential information.	Mim Dineen
Nov 2021	In review including pro bono legal advice and alignment with the Australian Privacy principles	People and Shared Services, Management Team and others
August 2022	Reviewed and approved	CEO