POL 4.2 Privacy and confidentiality

Scope

This policy conforms to the *Privacy Act 1988* Cth (Privacy Act), the *Health Records Act 2001* Vic, the *Privacy and Data Protection Act 2014 (Vic) including the Victorian Information Privacy Principles* and the *National Privacy Principles* which govern the collection, use and storage of personal information.

In February 2018 the Notifiable Data Breach Scheme also came into effect under Part IIIC of the Privacy Act. 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 and the Multi-agency Risk Assessment and Management (MARAM) Framework.

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.

Responsibilities

Compliance: All staff, volunteers and board members	**Review:** CARS Committee	**Approval:** Executive Officer

Definitions

Privacy: Includes privacy of the body – respect for physical person, privacy of the home, privacy from surveillance and privacy of personal information.

Personal information: *"... information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion." (Information Privacy Act 2000*)

Confidential information: means all information and data (and all copies and extracts made of or from such information and data), concerning the operations, dealings, organisation, business, finance, transaction, prospects, markets, designs, drawings, know-how and affairs of ARC Justice, and any information that ARC Justice designates as confidential.

Consent: Is an approval provided by a person. The individual must have the capacity to give consent. Consent must be informed, given freely, specific and current.

Privacy Officer: The privacy officer is responsible for overseeing all ongoing activities related to the development, implementation, maintenance, and adherence to the organization's policies and procedures covering the privacy, access, and personal information in compliance with federal and state laws.

Policy Statement

Right to Privacy

ARC Justice is committed to protecting and upholding the right to privacy for all including 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 information.

Clients will be provided with information regarding their right to privacy, what information is being collected, how their privacy will be protected and their rights in relation to this information. Where appropriate clients will be provided with written information regarding their privacy and the collection of information.

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 will sign an induction checklist and confirmation that includes reading this policy. Staff may in addition be asked to sign a more specific confidentiality agreement if their role requires.

The Corporate Services Manager has the role of the Privacy Officer to support and coordinate any known or possible privacy and data breaches.

Client consent

Personal information will only be collected with consent from an individual. Clients will be made aware of why information is being collected and specific consent sought to share this information.

Steps will be taken to ensure personal information collected is relevant, up-to-date and complete and not collected in an unreasonably intrusive way.

Clients will be made aware of and consent to:

- Who is collecting the information
- Why the information is being collected
- What it will be used for (including potential secondary uses)
- How the person can get access to the information
- Who else will have access to the information
- What the main consequences, if any, are for the person if they do not provide the information and who else the information might be given to.
- share de-identified information with funders and for statistical or secondary uses such as research.
- How long the information will be stored and the means of storage (ie secure electronic database, locked filing system)

Consent should be recorded, preferably in writing at the time the information is obtained. Consent may be revoked at any time.

Collection, use and management of personal information

ARC Justice will ensure that it meets its legal and ethical obligations as an employer and service provider and will follow the guidelines of the Australian Privacy Principals and the *Victorian Information Privacy Principles.*

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 information optimises privacy (eg using private interview rooms) and accuracy (eg collecting or confirming information with the client).

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 and imminent harm.

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

Staff will destroy or permanently de-identify personal information no longer needed and/or after legal requirements for retaining documents have expired.

If it is necessary to use or disclose personal information without consent a written note of the use or disclosure must be recorded.

Information regarding a client's health and/or medical treatment is only collected, recorded on file or communicated (in line with the Health Records Act 2001) if it directly relates to their case with ARC Justice and the client has provided their consent.

Use of information for secondary purpose

Clients must be informed of or given access the rights and responsibilities/ privacy statement that lists the potential secondary uses of personal information to ensure that information collected can be used for the secondary purposes of research, auditing and systematic advocacy.

Clients are required to provide consent to share information that includes any secondary purposes such as file audit and review, research and systemic advocacy.

Maintaining privacy and managing safety

Staff must not communicate, publish, release or disclose to any person information provided to them and/or ARC Justice in the course of their work likely to lead to the identification of a client or clients and/or identification of a client's legal problem, except:

- in the course of the delivery of services; or
- with the consent of the client where the client has the legal capacity to give consent; or
- with the consent of the client's Parent or Guardian or Attorney under Power of Attorney; or
- as required by law.

Unique identifiers from other organisations (i.e. Centrelink numbers) will not be adopted or assigned. These unique identifiers will not be disclosed to other agencies without specific consent except as required by law.

Staff should consider if it is appropriate to identify their service (e.g. CLC or HJ) or leave a message with a third party, unless there is prior consent.

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

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

Access to confidential information

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 information on intake and are informed of the process of how this can be carried out.

How we will maintain security of personal information

Irrespective of whether client information is stored electronically or in hard copy, ARC Justice will take all reasonable steps to protect the personal information. All client records will be kept securely and updated, archived and destroyed according to the service specific client records policies.

Client records will not be removed from the office unless necessary. Where client records are required to be removed from the office, a program specific client file movement register will be used. Client records that are taken out of the office must not be accessible to other people and must be secured in a locked bag/cabinet.

Client records will not be left in a car unless locked away and out of sight. No client information will be left unattended in a public or publicly accessible place.

Client records or data will not be taken out on memory sticks or CDs etc unless absolutely necessary and at a minimum password protected. Client records or data stored on a laptop taken outside the centre will also be password or otherwise security protected.

Staff must ensure all client documents are returned and stored securely as soon as possible.

How we will maintain data security

ARC Justice, with the support of the Information Communication Technology, will optimise data security under the following guidelines and resources the Australian Cyber Security Service's Essential Eight and Stay Smart Online

Privacy and data breaches

In the event of a breach of privacy ARC Justice will maintain the legal and ethical obligations. This may include informing the appropriate clients and agencies involved and where necessary reporting to funders and government bodies. Reportable breaches will be managed as per PRO 4.3 Privacy and data breaches.

Any staff misconduct during a breach of confidentiality will be managed as per PRO 8.4 Issues resolution and grievance.

How we will retain and destroy personal and confidential information

Generally ARC Justice aims to use client management systems to maintain client records for the necessary period (generally seven years). Where there is the need for hard copies client records will be stored securely for seven years.

Staff records are kept electronically (paper copies scanned) and will be kept during a staff member's employment and destroyed seven years after the staff member's termination.

Client and staff records will be destroyed following the necessary period in line with privacy requirements.

Publications and communication

Any information used for publications and communications will be used with informed consent. A privacy statement will be included in any ARC Justice website including collection of personal information.

Staff personal information

Personal information regarding ARC Justice staff, board members, volunteers and will be maintained and protected as per PRO 8.9 Staff records.

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 (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, health or sensitive information that is relevant to assessing and/or managing family violence risk can be shared between ISEs, provided:

- the information is not excluded
- sharing the information does not contravene another law, and
- applicable consent requirements have been met.

Housing Justice is an ISE 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 doesn't apply to the CLC. Information can be shared with consent, or without consent if an organisation reasonably believes it is necessary to lessen or prevent a serious threat to an individual's life, health, safety or welfare. Guidance has been issued on sharing to lessen or prevent a serious threat by the Office of the Victorian Information Commissioner and the Health Complaints Commissioner.

It is important to note that the word 'imminent' has been removed from the wording of *Privacy and Data Protection Act 2014* (PDP Act) and the *Health Records Act 2001* (HR Act). 'Serious' threats should take into account 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 (ie 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[1] – so it is most likely that any sharing of information regarding threats should be made to the police in the first instance.

Information Communication Technology (ICT) and privacy

ARC Justice, with the support of the ICT contractor will maintain data security. ICT Contracts include a privacy and confidentiality agreement and specific details about the approach to data security.

[1] Guidelines to the Information Privacy Principles (2011) 64.

Information barrier

ARC Justice is required to ensure an information barrier is maintained between the Community Legal Centre (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 10.1 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.

Monitoring and evaluation

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

Related policies, procedures and documents

This policy should be read in conjunction with:
Policies: POL 4.1 Regulatory compliance
Procedures: PRO 4.1 Maintaining regulatory compliance PRO 4.2 Access to confidential information PRO 4.3 Privacy and data breaches PRO 10.2 Information barrier PRO 12.8 Client file management CLC PRO 2.12 Client file management
Documents/ resources
Australian Privacy Principles Victorian Information Privacy Principles NACLC Risk Management Guide Multi-agency Risk Assessment and Management (MARAM) Framework Australian Cyber Security Services: Essential Eight Stay Smart Online Privacy and information security guideline for funded agency staff NFP Law guide to Privacy

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