

Privacy and Confidentiality Policy

Note on the Women's Housing Alliance Privacy Policy: *The Women's Housing Alliance (WHA) is auspiced by Juno. This means Juno's Privacy and Confidentiality Policy applies to all information collected, stored, and used by WHA.*

Purpose

The purpose of this policy is to make clear that the protection of privacy, as defined in the Privacy Act 1988 (Commonwealth) incorporating the Notifiable Data Breaches Scheme, Privacy and Data Protection Act 2014 (Vic), the Health Privacy Principles in the Health Records Act 2001 (Vic) and the Australian Privacy Principles, is a legal requirement and is relevant to Juno Services. This policy includes Juno requirements as an Information Sharing Entity (ISE) and Risk Assessment Entity (RAE) under the Family Violence Information Sharing Scheme (FVISS), as established by Part 5A of the *Family Violence Protection Act 2008 (Vic)*; the Child Information Sharing Scheme (CISS), as established under Part 6A of the *Child Wellbeing and Safety Act 2005 (Vic)*.

Juno is committed to complying with these laws, and to informing clients, staff and relevant others about privacy and confidentiality. This includes providing information relating to:

- Collecting personal information,
- Using and disclosing information,
- Recording and storing personal information,
- The rights and responsibilities of all stakeholders in terms of accessing and correcting information.
- The lawful instances when Juno may disclose personal and health information without consent of the person concerned.

Scope

This policy applies to all persons and all situations where personal and/or health information is sought by Juno Services, including all clients, Board and staff. This policy applies to all records, whether hard copy or electronic, containing personal information about an individual, of a sensitive personal nature.

Policy Statement

- Juno will meet its legal and ethical obligations as an employer and service provider to protect the privacy of people and the confidentiality of their information. Privacy and confidentiality will be maintained, unless otherwise required by law, duty of care or as enabled under relevant legislation.
- Juno ensures information is collected, handled and stored confidentially and securely by only allowing access to it by authorised Juno staff as appropriate, with personal and sensitive information recorded in keeping with the purposes of service provision.
- Juno ensures that all clients are provided with plain language information about this policy and their rights and responsibilities in relation to privacy. They are informed about how their

personal and sensitive information is collected, stored and shared, the extent and limitations of consent (where safe, reasonable and appropriate) under relevant legislation and how they can request access and make amendments to their personal records, including how to raise any concerns or complaints about the handling of personal information.

- Juno takes reasonable steps to ensure that the personal information collected is accurate, up to date and complete. Where misidentification of perpetrator or victim-survivor has occurred, a correction can be made within the record where appropriate and will occur in a timely manner. Where information is held by a third party, Juno will obtain consent before seeking or sharing information unless it is necessary to lessen or prevent harm, or in accordance with the Child and Family Violence Information Sharing Schemes.
- Juno requires all staff to be consistent and careful in the way they manage what is written and said about clients, and how they decide who can see or hear this information. Information collected, stored and shared highlights victim-survivor strength and resistance, and perpetrator behaviour, tactics and impact.
- Juno ensures precautions are taken to prioritise victim-survivors' confidentiality when providing services in rural/regional locations or within close-knit social/cultural communities.
- Juno ensures the use of client data for reporting, systemic advocacy or continuous improvement is de-identified, aggregated and not traceable to any particular individual, family or staff.
- People accessing Juno have the right to refuse to provide information which is not essential to service provision, however, Juno is required to collect minimum information in order to provide a service, which is explained to the client.
- Juno does not sell any personal information to any third party.

Juno collects information from the following individuals and groups

Clients

Juno collects personal information on or about people who access our services. Juno will make all endeavours to collect information through referrals and the person directly, where this is not possible the client will be informed about the information that has been collected to ensure relevancy and accuracy of information gained through a third party.

Juno collects sensitive and health information when necessary for providing services or is a requirement of government funding, or during activities related to service delivery.



Additional information necessary for service provision is also collected. This includes the need for Juno to assess eligibility for entry to, or support from, specific programs or services. Personal information that Juno receives will be stored only if the information is reasonably necessary for the organisation's functions or activities and if it is relevant for client's safety. Otherwise the information will be securely destroyed or de-identified if it is reasonable and lawful to do so.

Staff

Juno collects the personal information of people who seek to be, are, or have been employed with us. This includes information about recruitment and selection, employment, terms and conditions of employment, performance, discipline and resignation.

Juno collects the personal information of people who seek to be, are, or have worked with the organisation as volunteers. This may include information about recruitment and selection, work arrangements, performance, discipline and resignation.

A minimum data set is gathered from students in order to meet the requirements of the formal agreement with the student's educational institution, as well as Juno standard employee information.

Donors, Partners and other Stakeholders

Juno collects personal information for the purposes of processing donations, fund raising, keeping supporters and donors informed of our work, raising awareness, thanking and acknowledging our donors and supporters, conducting research into supporter attitudes and desires, and for internal reporting purposes.

Juno uses and discloses information in the following ways

Clients

Client information is not normally disclosed to other organisations or individuals without consent. An exception to this may be where Juno is required to do so by law including under the Children, Youth and Families Act, Child and Family Violence Information Sharing Schemes, or government funding agreements. Juno may use deidentified information for the evaluation (planning and research) of its services.

Staff



Information about staff is not normally disclosed to other organisations or individuals without their consent, unless we are required to do so by law, government requirements or government funding agreements.

In a case where personal information is supplied to or collected by contractors who perform specific tasks directly on our behalf (for example mailing houses), contractors are required to sign a privacy agreement with Juno which obliges the contractor to comply with Juno's Privacy Policy, the Privacy Act and the Australian Privacy Principles.

Donors, partners and other stakeholders

From time to time, Juno will acknowledge and thank supporters and donors in our publications unless donors request that this not happen.

Funding bodies

Information provided to funding bodies is both de-identified and aggregated to protect anonymity and provide general descriptive information. Whenever possible, clients are informed of the requirement to pass on information and the nature of the information.

Juno will, from time to time, provide de-identified and aggregated client data to funding sources other than government to support funding submissions. Such information may also be used to report on the success of a funded project. In principle, informed consent will be sought wherever possible to maximise client choice to participate in such activities.

Accessing and correcting info

Clients have a right to apply to access all information which Juno collects and stores about them, and a right to advise of any errors of fact, or update details as required. If errors are identified, Juno will note the error in the client file, ensure to include that this information has been provided by the client, and the change has been requested by the client. In circumstances where a victim-survivor is misidentified as a perpetrator, Juno will note in the client file that misidentification has occurred, and to complete appropriate risk assessment and risk management processes applied to rectify exacerbation of risk.

- All clients are provided with information about how to access their information. Only in exceptional circumstances where Juno reasonably believes denial of access to records may lessen or prevent a serious threat to an individual's welfare, unreasonable impact on the privacy of other individuals or a threat to public health and safety, will access to records be denied.

- Staff, donors, partners and/or other stakeholders can view the information Juno holds on them and have the right to correct any errors of fact in the recorded information.
- Juno is committed to ensuring donors, partners and other stakeholders retain control over the communications we send to them. They may decline to receive publications or other communications from Juno at any time.
- Clients, donors and supporters all have a right to make a complaint regarding the handling of their personal information should they wish to do so.

Use of Juno information by employees

Employee access to and use of confidential information is limited to work-related activities. Access, use of, or disclosure for any other purposes is prohibited without proper authorisation, unless required by law. The internal systems of Juno must not be used to access information for personal benefit or interest, or that of any employee's family, friends, colleagues, or of any public figure.

Breaches of confidentiality, access and disclosure of information will be treated as a serious misconduct issue.

Juno considers the following examples of confidential information:

- a. Lists of clients and contact details
- b. Supporter information, contact details, donation history and financial information
- c. Any financial or costing information
- d. Research data or papers not publicly released
- e. Information about new program and/or service development
- f. Employee remuneration
- g. Details of tenders
- h. Marketing /communication plans
- i. Intellectual property or other processes unique to the employer
- j. Terms of business

Exceptions

Juno upholds the right of individuals to have their privacy and confidentiality recognised and maintained. Relevant policy and legislation will be followed in circumstances where the right to privacy may be overridden by other considerations. These may include:

- Consent has been provided by client, carer or an authorised person
- Under privacy law for the primary purpose or related secondary purpose for which it was collected
- Where necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety.

- In compliance with a court order, subpoena, summons or as required by law
- For risk assessment and/or risk management purposes where serious threat is present, or the information relates to the safety or wellbeing of a child, as required by the Family Violence Information Sharing Scheme and the Child Information Sharing Scheme.
- In compliance with the Notifiable Data Breach Scheme

Data Security

Personal information held by Juno will be protected against loss, unauthorised access, use, or disclosure by means of reasonable technical, physical, and administrative safeguards including:

- Using passwords to prevent unauthorised access and use of computers and relevant software;
- Establishing access levels to restrict access so that only relevant staff have access to certain information;
- Ensuring information is transferred securely;
- Installing virus protections and firewalls;
- Locking filing cabinets and other areas in which personal information is stored;
- Ensuring documentation containing personal or confidential information is securely destroyed;
- Not storing personal information in public areas;
- Positioning computer terminals so that they cannot be seen or accessed by unauthorised people or members of the public.
- When working from home/private residence staff will ensure all equipment and documentation is held in a secure place where no other individual will have access. All electronic and verbal communication will be conducted in a secure manner where conversations cannot be overheard.
- All contractors employed by Juno Services, sign a confidentiality agreement before any works can commence on premises.

Privacy Breach

As an organisation funded by the Victorian Department of Families, Fairness and Housing (DFFH), Juno is required to immediately notify DFFH when becoming aware of a breach of the privacy of a client, or a possible breach, as defined under the Privacy and Data Protection Act 2014 (Vic) or the Health Records Act 2001 (Vic).

Privacy Breaches must be reported within one business day via the DFFH Privacy Incident Report eform available [here](#).

Note that such a breach may also need to be reported under the Notifiable Data Breaches Scheme and/or the DHHS Client Incident Management System (CIMS). The client will be notified by the Chief Executive Officer as soon as appropriate.

Lodging a complaint

Privacy and confidentiality related complaints and breaches are effectively dealt with through fair and consistent procedures. Juno adheres to the Complaints and Feedback Policy and relevant procedure to decide what action will be taken to resolve privacy complaints. All privacy and confidentiality complaints will be responded to within 30 days.

If unsatisfied with the response, the complaint can be made by the client to the Victorian Information Commissioner (OVIC), the Health Complaints Commissioner (HCC) or the Office of the Australian Information Commissioner (OAIC).

Responsibilities

- | | |
|------------|---|
| Leadership | <ul style="list-style-type: none"> • Maintain a system for privacy and data quality and security related risk oversight. • Ensure all confidential information is appropriately collected, stored, accessed and used. • Implementation of this policy and monitor employee adherence to the policy • Ensure the policy is updated as per the regular policy review cycle or if there are changes to the compliance environment. • Manage and respond to breaches of privacy breaches and all complaints are addressed quickly and transparently. |
| All Staff | <ul style="list-style-type: none"> • Always abide by this policy, associated procedures and legislation. • Notify clients about their rights and responsibilities with respect to privacy and confidentiality. • Explain to clients the privacy and confidentiality limitations defined by law, including the Child and Family Violence Information Sharing schemes. • Inform line manager or direct supervisor of any issues relating to privacy and confidentiality breaches. |

Relevant legislation and external documents

- Privacy Act 1988 (Commonwealth)
- Privacy and Data Protection Act 2014 (Vic)
- Health Records Act 2001 (Vic)
- Charter of Human Rights and Responsibilities Act 2006 (Vic)
- Australian Privacy Principles 2013 (Amended 2014)
- Family Violence Protection Act 2008 (Vic)
- Family Violence Protection (Information Sharing and Risk Management) Regulations 2018
- Family Violence Multi-Agency Risk Assessment and Management Framework 2018

- Family Violence Information Sharing Scheme Ministerial Guidelines
- Child Wellbeing and Safety Act 2005 (Vic)
- Child Wellbeing and Safety (Information Sharing) Regulations 2018
- Child Information Sharing Scheme Ministerial Guidelines
- Code of Practice: Principles and Standards for Specialist Family Violence Services for Victim-Survivors
- [DFFH Reporting Privacy Incidents](#)

Related documents

- Child and Family Violence Information Sharing Scheme Procedure
- Feedback and Complaints Brochure
- Clients Rights and Responsibilities Brochure
- Protecting your right to Privacy and Confidentiality Brochure
- Complaints Compliments and Feedback Policy
- Privacy and Confidentiality Procedure
- Code of Conduct

Definitions

Health information	Any information or opinion about: <ul style="list-style-type: none"> • The physical, mental or psychological health of an individual. • A disability of an individual. • An individual's expressed wishes about the future provision of health services to the individual. • A health service provided, or to be provided, to an individual, that is also personal information.
Consent	Permission for something to happen, or agreement to do something, after being provided all relevant information. Consent is based on a person's capacity to understand, retain, use or weigh and communicate their decision, views and needs in some way.
Confidentiality and Privacy	Implies the respect for and the preservation of an individual's right to privacy of any personal information, either oral or written. It is the understanding that any information offered within the working relationship will not be disclosed to anyone outside that relationship without the informed consent of the individual providing the information, unless it is necessary, reasonable and appropriate to prevent any serious harm or as required under relevant legislation.
Client	Adult and child victim-survivors are sometimes referred to as 'clients' of specialist family violence services.
Personal information	Any information that may identify a person. Personal information includes a person's name or address, where a person works, information contained in risk assessments, interactions between client and staff and CCTV footage recorded at a Juno site or service, and any other information that could reasonably identify them.
Sensitive information	Any information about a person's experiences or circumstances that is of a private nature but is relevant to the service being provided. This includes information or opinion about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association,



membership of a trade union, gender identity, sexual preferences or practices, criminal record.

An organisation can only collect sensitive information in restricted circumstances or with consent. Sensitive information may be associated with trauma and must be treated with mindfulness and respect.

Staff

Refers to all persons working within Juno including paid, unpaid, students, volunteers and contractors.