Privacy Confidentiality and Consent Procedure IMS-P2-PR1

1. Procedure objective and overview

1.1 Privacy

This procedure outlines how Ruah manages personal information in accordance with the Privacy Act, 13 Australian Privacy Principles, and Notifiable Data Breach Scheme.

This procedure applies to all personal and sensitive information collected, received, or held by Ruah about clients, donors, job applicants, volunteers, contractors, and employees (for purposes unrelated to their employment agreement).

1.2 Confidentiality and Informed Consent

This procedure outlines the process of providing information for individuals about service options and disclosure of personal information, and the extent and limits of confidentiality, so they can make informed decisions in their interest.

2. Prerequisite knowledge and skills

- Orientation
- Code of Conduct IMS-P3-PR2-TOR1
- Technology User Declaration IMS-P1-PR6-F2

3. Procedure

3.1 Privacy - Australian Privacy Principles

The Privacy Act, which contains 13 Australian Privacy Principles, regulates how personal information must be managed to protect an individual's privacy. Ruah complies with these in the following ways.

3.1.1 Open and transparent management of personal information

Ruah manages personal information in an open and transparent way by having:

- procedures and systems that enable compliance with the Australian Privacy Principles
- a readily available Privacy Statement on Ruah's website, in client welcome packs and in our offices that clearly outlines the kinds of information Ruah collects, how we collect the information, and the purposes for collecting the information.

3.1.2 Anonymity and pseudonymity

Whenever it is lawful and practical, individuals must be given the option of not identifying themselves while dealing with Ruah. Options for anonymity include using an alias.

If a new client requests anonymity, staff in the initial meeting will consider whether Ruah is able to provide a quality service if the client is anonymous. If staff are satisfied that a quality service can be provided while the client is anonymous, staff will explain the options, including using an alias. Staff will explain the consequences of anonymity (e.g., difficulty contacting the client in emergencies, inability to supply support letters), and the limits of using an alias to protect anonymity. Staff must discuss these instances with their line manager.

3.1.3 Collection of personal information

Staff must only collect **personal information** that is necessary for, or directly related to, Ruah's work. Where information is collected for research and /or evaluation purposes additional consents will be sought. Personal information will be collected from the individual directly (or if information is received by referrals, the information will be checked with the client). In addition, staff will only collect **sensitive information** with the individual's informed consent.

3.1.4 Unsolicited personal information

When Ruah receives unsolicited personal information, the staff member who receives the information must decide whether the information is necessary for, or directly related to, Ruah's work. If the information could have been collected as part of Ruah's core work, the other privacy principles apply to that personal information.

If the information couldn't have been collected under Ruah's normal work, then steps must be taken to either destroy the information or de-identify it so that it no longer contains personal information, unless the information is contained in a Commonwealth record.

3.1.5 Notification of the collection of personal information

Either at the time or before Ruah collects information, staff must ensure that the individual is aware that Ruah collects personal information about them.

All client referral/assessments, recruitment advertisements, requests for donations, and Ruah's website must notify individuals that Ruah collects personal information.

3.1.6 Use or disclosure of personal information

Personal information about an individual that is collected for one purpose (e.g., engagement in a Ruah program, making a complaint, or a job application) must not be used or disclosed for another purpose (e.g., soliciting donations), except when the individual would reasonably expect it or when they provide consent.

Disclosure of personal information about an individual is permitted when:

- there is a serious and imminent threat to an individual's or other's life, health, or safety;
- the disclosure is authorised or required by law (please refer to Responding to Subpoenas and External Requests for Information IMS-P1-PR2-WI2); or

- the disclosure relates to significant criminal behaviour, and is made to authorities with responsibility for dealing with such behaviour, and disclosure is not outweighed by other privacy principles;

When personal information is used or disclosed, in accordance with the above, a written note of the use or disclosure must be made in the individual's record. Any staff member involved in making this disclosure should not make the decision to do so alone, but should liaise with their line manager, on-call or other senior staff member.

3.1.7 Adoption, use, or disclosure of government-related identifiers

Ruah uses government-related identifiers (e.g., driver license, passport) to confirm the identity of prospective employees. This personal information is handled in accordance with the other privacy principles.

3.1.8 Quality of personal information

Ruah must take reasonable steps to ensure that all personal information it holds is accurate, up-to-date, and complete. Regular client file audits and personnel record checks assist Ruah to meet this requirement.

All staff are responsible for updating the records they maintain to reflect changes. If some personal information is likely to change regularly, staff must check the records periodically to ensure that they are accurate, up-to-date, and complete.

3.1.9 Security of personal information

Ruah takes reasonable steps to protect personal information from:
- misuse, interference, and loss
- unauthorised access, modification, or disclosure.

(See Ruah's ICT Procedure IMS-P1-PR6 for more information).

Ruah takes reasonable steps to de-identify or destroy personal information when:
- it is no longer needed for the purpose for which it was collected and allowed to be used or disclosed
- the information is not contained in a Commonwealth record
- Ruah is not legally required to retain the information.

To ensure the security of personal information:
- Client and personnel records and other forms of personal information must only be accessed by authorised staff who require access for their duties.
- **Unauthorised access may result in termination of employment with Ruah.** It may constitute a Notifiable Data Breach that has legal implications (see 3.2, page 5).
- All records containing personal information must be destroyed securely or de-identified in accordance with the Record Retention and Disposal Schedule IMS-P1-PR6-RE1.

3.1.10 Access to personal information

Ruah provides access to an individual's personal information, on request, unless an exception applies (as outlined below in 3.1.10.3).

3.1.10.1 Verify identity

Ruah must be satisfied that a request for personal information is made by the individual concerned, or by another person who is authorised to make a request on their behalf (e.g. a legal guardian or authorised agent). If Ruah gives access to the personal information of another person, this could constitute an unauthorised breach of privacy.

3.1.10.2 Timely response

While in practice it is likely to be much quicker, Ruah must respond to a request for access within 30 calendar days of receipt of the request. Ruah must respond by giving access to the requested information, or by notifying refusal to give access. If there is a justifiable reason for delay (e.g. need to clarify scope of request, or to locate and assemble the requested information, or to consult a third party), Ruah must contact the individual to explain the delay and provide an expected timeframe for finalising the request.

3.1.10.3 Exceptions to requests for access

The Australian Privacy Principles outline circumstances when a request for access can be declined, including when:

- the information relates to a current or former employment relationship or the individual's employee record;
- the information relates to existing or anticipated legal proceedings between the organisation and the individual, and would not be accessible by the process of discovery in those proceedings
- giving access would reveal the intentions of the organisation in relation to negotiations with the individual in such a way as to prejudice those negotiations
- giving access would have an unreasonable impact on the privacy of other individuals
- giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety.

If a decision to refuse access is made, Ruah must provide the individual with a written notice that sets out the reasons for the refusal and the complaint mechanisms available to the individual. The individual may have a right to complain to the Information Commissioner under the Privacy Act. After investigation, the Commissioner may determine that Ruah failed to comply with Australian Privacy Principles and require that Ruah give access.

3.1.10.4 Method of access

Ruah must give access to personal information in the manner requested by the individual if it is reasonable and practical to do so. The manner of access may include by email, phone, in person, hard copy, or electronic record.

3.1.11 Correction of personal information

Ruah must take reasonable steps to correct personal information it holds about an individual if the individual requests that it be corrected. When personal information is used or disclosed, staff may need to correct it before use or disclosure if it is satisfied the information is inaccurate, out-of-date, incomplete, irrelevant, or misleading.

3.1.12 Australian Privacy Principles that are not relevant for Ruah

- Ruah does not need to comply to Australian Privacy Principles related to: Direct marketing - because Ruah does not engage in direct marketing.
- Cross-border disclosure of personal information because Ruah does not disclose personal information to any overseas recipient.

3.2 Privacy - data breaches

3.2.1 What is a data breach?

A data breach occurs when personal information held by Ruah is lost or accessed or disclosed by an unauthorised person or in an unauthorised manner. A data breach may be caused by malicious action (by an external or internal party), human error, or a failure in information handling or security systems.

Examples of data breaches include:
- loss or theft of physical devices that contain personal information (e.g. laptops)
- unauthorised access to personal information by an employee
- inadvertent disclosure of personal information due to human error, e.g. an email sent to the wrong person
- disclosure of an individual's personal information to a scammer, due to inadequate identity verification procedures

A data breach may result in serious harm to the individual whose personal information was breached. Examples of serious harm include:
- financial fraud including unauthorised credit card transactions or credit fraud
- identity theft causing financial loss or emotional and psychological harm
- physical harm or intimidation

3.2.2 What is a notifiable data breach?

The Notifiable Date Breach Scheme in Part IIIC of the Privacy Act requires Ruah to notify affected individuals and the Privacy Commissioner when:
- There is a data breach; and
- The data breach is likely to result in serious harm to any of the individuals to whom the information relates; and
- Ruah has been unable to prevent the likely risk of serious harm with remedial action.

3.2.3 What to do if there is <u>any</u> breach of privacy or data breach

If any data breach occurs, it must be treated as a critical incident and escalated and investigated in accordance with Ruah's Risk Management Procedure IMS-P1-PR2. Staff must report the breach to their Manager, who will alert the Executive Managers, so Ruah can respond to the breach as required by the Privacy Act.

3.3 Informed consent

3.3.1 Consent before engagement

Consent and confidentiality are fundamental rights that must be available to all people accessing services. Staff obtain informed consent before collecting information, disclosing personal information, or providing services.

To provide informed consent, clients need to understand:

- what services Ruah can provide
- conditions for accessing Ruah's services, including client rights and responsibilities
- how personal information is managed by Ruah
- the extent and limits of client confidentiality
- the right to change and withdraw consent at any time, and
- the consequences of withdrawing consent

Ruah provides a voluntary service, and as such treatment and care can only occur once the client is fully aware of the potential risks and benefits associated with the type of service they are agreeing to take part in. A client may decline to provide consent; however, this may result in Ruah being unable to deliver a full service to them. Ruah may be able to provide a basic needs and information provision only service if a client does not consent to have any personal details collected and wishes to remain anonymous.

The process of obtaining client's informed consent includes appropriate involvement of carers, other service providers, and others nominated by the client, in assessment and support.

Additionally, clients must be provided with enough information to make an informed decision and must also be capable to do so. Capability to provide informed consent includes, for example, clients who do not have diminished capacity requiring a Guardian or Power of Attorney and must be over 18 years of age or assessed as a mature minor.

3.3.2 Consent for sharing information

Staff explain how Ruah manages personal information securely, and the extent and limits of confidentiality (see below).

Staff obtain written permission before any personal information is provided to or obtained from another Ruah program or external agency. Individuals must give signed permission for Ruah staff to disclose or share information with any other Ruah service provider, agency or program, the public, or family members.

3.4 Extent and limits of client confidentiality

Staff must inform clients about the extent and limits of client confidentiality. Information received in confidence must not be disclosed without written consent unless there are compelling reasons to do so. Staff have a duty of care and in some cases a legal

responsibility to inform relevant parties to ensure the safety and wellbeing of individuals and the public, as outlined under the Australian Privacy Principles (see Page 2, 3.1.6).

3.5 Mature minors and consent

Under the WA Mental Health Act 2014 a young person in Western Australia under the age of 18 years can be considered competent to provide their consent to be referred to and to participate in a mental health service.

The number of young people requiring such assessment by Ruah is relatively small and the assessment, undertaken using the Gillick Principle, is considered a specific skill set. Ruah recognise that to meet the requirements of all legislative and client expectations in this area, the assessment of a young person's ability to make these decisions are largely subjective. Therefore, all such cases must be assessed and signed off by the team coordinator.

In determining if a person aged 16 to 18 years of age can provide consent, Coordinators need to consider:

- the age of the child (anyone aged under 18 years is legally a child)
- the child's history of making their own decisions
- the length of time the child has been living independently (if applicable)
- the child's cognitive functioning, i.e., presence or absence of any decision-making or psychiatric impairment, or drug/alcohol use that may affect the child's ability to understand the implications/impact of decisions being made
- the child's level of understanding of the matter and the likely consequences of any decisions made.
- what the child is consenting to (e.g. consenting to discuss their personal relationship problems versus to consenting to medical treatment or to live away from home).

3.6 Legal guardianship and consent

Some clients have an enduring power of attorney, enduring power of guardianship, or an administration order through the State Administrative Tribunal. Staff must ask clients, on entry to a service, if this is the case.

If power of attorney or guardianship or administration order are identified, consent forms are required to be completed by the nominated guardian.

Consent forms signed by clients on a Guardianship Order are not considered legal documents because the individual has been assessed as incapable of providing informed consent.

3.7 Additional consent documentation required

Some Ruah programs have contractual requirements to complete consent documentation in addition to Ruah's Client Consent Form IMS-P2-PR1-O1 that is required for all Ruah programs.

3.8 External advocacy agencies

At initial engagement, staff must inform case managed clients about the external sources of support and advocacy available to them when making a complaint. This information is included in the Client Welcome Pack and Carer Welcome Pack.

4. Definitions

Personal Information	Information about an identified individual, or an individual who is reasonably identifiable. Common examples are an individual's name, signature, address, telephone number, date of birth, medical records, bank account details, and opinion about the individual (e.g., notes in staff or client records).
Sensitive Information	A type of personal information that includes information about an individual's race or ethnic origin, political opinions, memberships of a political association, professional or trade association or trade union, religious or philosophical beliefs or affiliations, sexual orientation or practices, gender identity, genetic or biometric information, health information, and criminal record.
Health Information	Any information about an individual's health, and any other information collected by a health service provider.
Informed consent	The process for providing clear understandable information for individuals about service options and disclosure of information, so they can make decisions in their interest; obtaining permission before providing services or disclosing personal information; permission granted with full knowledge of possible risks and benefits.
Confidentiality	The legal and ethical obligation not to disclose information to a third party when that information has been provided in confidence.
Confidential information	Information about an individual that the individual can reasonably expect not to be disclosed and which has not already been made public

5. References

Office of the Australian Information Commissioner https://www.oaic.gov.au

6. Related Documents

Document Title	Document ID
Code of Conduct	IMS-PR2-TOR1
Corporate Governance Policy	IMS-P1
ICT Procedure	IMS-P1-PR6
Technology User Declaration	IMS-P1-PR6-F1
Service Delivery Policy	IMS-P2
Clinical Governance Procedure	IMS-P2-PR6
Risk Management Procedure	IMS-P1-PR2
Record Retention and Disposal Schedule	IMS-P1-PR6-RE1

Client Consent Form	IMS-P2-PR1-F1
Responding to Subpoenas and External Requests for Information	IMS-P1-PR2-WI2
Privacy Confidentiality and Consent Work Instruction	
Management of Complaints Work Instruction	IMS-P2-PR6.2-F2

7. External obligations

Privacy Act, 1988
Privacy Amendment (Enhancing Privacy Protection) Act 2012
Privacy Amendment (Notifiable Data Breaches) Act 2017