

Shoalhaven Womens Resources Group Ltd – ROCC for Women

Policy Name	Confidentiality & Privacy
Policy Section	Client Services
Version	Version 3
ASES Standard	Standard 2: Governance <ul style="list-style-type: none"> 2.3 Data and Knowledge Management Standard 6: Communication <ul style="list-style-type: none"> 6.1 Communication Standard 8: Consumer Outcomes <ul style="list-style-type: none"> 8.1 Consumer and Community Engagement
Date of Implementation	May 2022
Date of Review	May 2024

Policy:	<p>Shoalhaven Womens Resource Group (SWRG) requires Board members, staff, students, contractors and volunteers to respect and maintain the confidentiality of individuals and of the company's business.</p> <p>SWRG is committed to protecting and upholding the right to privacy of clients, staff, volunteers and Board Members. In particular SWRG is committed to protecting and upholding the rights of our clients to privacy in the way we collect, store and use information about them, and the services provided to them.</p> <p>SWRG will follow the guidelines of the <i>Australian Privacy Principles, Privacy and Personal Information Protection Act 1998</i> and the <i>Health Records and Information Privacy Act 2002</i> in its information management practices.</p>
Scope:	All SWRG Staff, Board Members, volunteers and students
Related policies or other documents	<p>SWRG Client Records Policy</p> <p>Australian Privacy Principles</p> <p>Privacy and Personal Information Protection Act 1998</p> <p>Health Records and Information Privacy Act 2002</p> <p>SWRG Client Consent to Share Information</p> <p>Code of Conduct and Confidentiality Agreement</p> <p>Clients Rights and Responsibilities</p>

Procedure

Key Steps	Procedure
SWRG responsibility	<p>SWRG will only collect personal information required for the service provided. This includes meeting legal requirements.</p> <p>All SWRG staff, students, volunteers and Board members will sign a Code of Conduct and Confidentiality Agreement upon commencement of their engagement with SWRG.</p>
Client responsibility	<p>All clients are expected to maintain confidentiality about and respect the privacy of other service users. This will be explained to clients by the case worker upon their engagement with the service.</p> <p>All clients will be given a copy of the "Client Rights and Responsibilities" statement.</p> <p>The Client Rights and Responsibilities statement will be displayed in all SWRG premises.</p>



<p>Staff responsibility</p>	<p>Staff will discuss the “Client Consent to Share Information” form with clients as soon as appropriate after the client engagement. Clients will be asked to complete and sign this consent form, which will be scanned and stored with their electronic client files.</p> <p>Staff will not discuss client’s details with anyone outside the organisation without the client’s permission, preferably in the form of signed consent. The only exceptions to this are:</p> <ul style="list-style-type: none"> • If client information is subpoenaed • If there is a real fear for the safety of the client or of another person <p>Exceptions will be discussed with the client whenever possible.</p>
<p>Information Protection Principles (Privacy and Personal Information Protection Act 1998)</p>	<p>SWRG abides by the following Information Protection Principles:</p> <ol style="list-style-type: none"> 1. Lawful: personal information can only be collected for a lawful purpose that is directly related to the agency’s function or activities. 2. Direct: personal information can only be collected directly from the client, unless the client has authorised collection from another person. 3. Open: the client will be informed that the information is being collected, why it is being collected and who will be storing and using it. The client will also be informed about how they can access their personal information, if the information is required by law or is voluntary, and any consequences that may apply if they decide not to provide it. 4. Relevant: the personal information collected must be relevant, accurate, complete and up-to-date. 5. Secure: personal information must be stored securely, kept no longer than necessary and disposed of appropriately. It should be protected from unauthorised access, use or disclosure. 6. Transparent: the client must be provided with details about what information is being stored, why it is being stored and any rights they have to access it. 7. Accessible: the client must be allowed access to their personal information without excessive delay or expense. 8. Correct: the client must be allowed to update, correct or amend their personal information where necessary. 9. Accurate: the agency will ensure that personal information is relevant, accurate, up-to-date and complete before using it. 10. Limited: personal information can only be used for the purpose it is collected or for a directly related purpose, unless the client has given consent or to prevent or lessen a serious or imminent threat to any person’s health or safety. 11. Restricted: personal information can only be disclosed in limited circumstances if a client has given consent, or if disclosure is necessary to prevent a serious and imminent threat to any person’s health or safety. 12. Safeguarded: sensitive personal information cannot be disclosed without the client’s consent, unless it is necessary to prevent a serious and imminent threat to any person’s health or safety.
<p>Breaches of confidentiality</p>	<p>Breaches of confidentiality will be taken seriously and grievance procedures will be initiated when necessary.</p>