Title Privacy and Confidentiality Policy and Procedure

Sections	Community Services
Risk	Medium
Distribution	All Staff, Clients

Co.As.It. is committed to its responsibility of protecting the personal information and maintaining confidentiality of all the consumers, employees, volunteers and other individuals associated with the company. Protection of privacy and the need for confidentiality is fundamental in providing a high quality service and it is an obligation under the Privacy Act 1998 (Cth) and the Australian Privacy Principles (APPs).

For the purpose of this policy and procedure, 'employee' includes volunteers and contractors of Co.As.It.

This policy sets out the practices adopted by Co.As.It. to ensure open and transparent management of personal information and compliance to the APPs which are set out in Schedule 1 in the Privacy Act 1998. http://www.comlaw.gov.au/Details/C2014C00076/Html/Text#_Toc382303234

Definitions

Personal information – is defined as any 'information or an opinion about an identified individual, or an individual who is reasonably identifiable'.

Sensitive information – is a subset of personal information and is defined as information or an opinion (that is also personal information) 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; sexual preferences or practices; or criminal record.
- Health information about an individual.
- Genetic information (that is not otherwise health information).
- Biometric information that is to be used for the purpose of automated biometric verification or biometric identification.
- Biometric templates.

Notifiable data breach – where there has been unauthorised access or disclosure of personal information it holds, or such information has been lost in circumstances where that's likely to lead to unauthorised access or disclosure; and a reasonable person would conclude that such access or disclosure would

be likely to result in serious harm to any of the individuals to whom the information relates.

Confidentiality protects personal information from unauthorised use or disclosure by placing a responsibility on the individual who obtains this information to keep it private. Confidential information is sensitive and is protected by law and by Co.As.It. policies. Confidentiality is a matter of concern for all persons who have access to personal information about consumers and employees. Individuals who are authorised to access consumer and employee information must read and comply with this policy.

Privacy refers to a person's right to keep certain information private. Co.As.It. employees will respect an individual's right to privacy by following practices that ensure the information remains confidential.

Principle 1: Open and transparent management of personal information

Co.As.It. understands its duty to protect the personal information of consumers and employees. Co.As.It. maintains confidentiality by restricting access of personal information to authorised persons, entities and processes at authorised times and in an authorised manner. Co.As.It. employees work under professional codes of conduct and ethical guidelines that require them to adhere to their 'duty of confidentiality'. Employees will be responsible for their misuse or wrongful disclosure of confidential information and their failure to safeguard their access code or other authorisation access to confidential information. Any breach of confidentiality by employees will be treated as a disciplinary matter. All employees are required to sign the Privacy and Confidentiality Agreement Form upon receiving training on this policy during induction.

Co.As.It. will maintain an up to date policy regarding the management of personal information. Co.As.It. will ensure that copies of this policy are made available to consumers and employees and will also provide copies of the policy upon request.

Principle 2: Anonymity and pseudonymity.

Individuals have the right to not identifying themselves, or using a pseudonym when making initial enquires regarding the services available at Co.As.It. However, this does not continue once the individual has engaged in services with Co.As.It., as it may be impracticable for Co.As.It. to deal with consumers that have not identified themselves or have used a pseudonym.

Principle 3: Collection of solicited personal information

Personal Information: will only be collected if it is reasonably necessary for one or more of Co.As.It.'s functions or activities. Disclosure of information will only be for the purpose for which it was collected. Personal information will only be used or disclosed for a secondary purpose when a consumer has given consent to use the information, or if the information is related to the primary purpose of the collection of the information.

Sensitive Information: relates to information about an individual's religious beliefs, racial or ethnic origin, sexual orientation, membership of a political association, criminal records, health information, etc. Sensitive information will only be collected when a consumer has given consent and when the information is necessary for one or more of Co.As.It.'s functions or activities. Co.As.It. may be required to collect sensitive information if it is required under an Australian law, a court/tribunal order or if a permitted health situation exists.

When collecting personal and sensitive information Co.As.It. will ensure;

- That information has been collected by lawful and fair means;
- Information has been collected with consent;
- Consumers have been made aware of their right to withdraw consent upon negotiation with Co.As.It;
- Collection of information is limited to only the amount of information which is necessary for Co.As.It. to perform its functions;
- Where information has been obtained from a third party, that it has been obtained by lawful and fair means.

Principle 4: Dealing with unsolicited personal information

In the event that Co.As.It. receives personal information regarding a consumer or employee which was not solicited by Co.As.It. then Co.As.It. will determine whether or not the information could have been collected in accordance to Principle 3. If it is determined that Co.As.It. could not have collected the information in a manner that is compliant with Principle 3 then the information will be destroyed.

Principle 5: Notification of collection of personal information

- Co.As.It. will clearly state the purpose for the collection of personal information.
- Where consumers or employees refuse to provide the necessary information, Co.As.It. will clearly state the consequences of not providing such information.
- Consumers of Co.As.It.'s Community Services programs are made aware of the agencies that Co.As.It. may need to disclose personal information for the delivery of the program. Consumers are asked to

sign a consent form authorising Co.As.It. to share information with these agencies.
- Co.As.It. will advise if the purpose of the collection of the personal information is required by or under an Australian law or court/tribunal.

Principle 6: Use or disclosure of personal information

- Co.As.It. may disclose personal and sensitive information to employees, for the specific purpose of administration and for the appropriate case management of its consumers.
- Personal and sensitive information can only be used for a secondary purpose when informed consent is obtained or when it relates directly to the primary purpose for which it was collected.
- Co.As.It. is required to release personal information if the information has been requested by or under and Australian law, a court/tribunal order or enforcement related activities conducted by or on behalf of an enforcement body. Co.As.It. is required to make a written note when information has been disclosed for an enforcement related activity.
- Co.As.It. may be required to release personal information during medical emergencies to ensure the health and safety of consumers and employees.

Principle 7: Direct marketing

- Personal and sensitive information will not be used or disclosed for the purpose of direct marketing unless the information has been collected from the individual, and the purpose has been clearly explained to the individual and they have consented to its use.
- Employees will obtain consent from the consumer prior to publishing photos, stories or other personal information. Consent will be obtained by asking the consumer to sign the Consent Form (Promotional Photos/Video).

Principle 8: Cross-border disclosure of personal information

- Prior to releasing information to an individual overseas, Co.As.It. will take all reasonable steps to ensure that the individual does not breach the Australian Privacy Principles. This is with the exception of where Co.As.It. is required to release the information by or under an Australian Law, a court/tribunal order, an enforcement agency or the information is required by or under an international agreement relating to information sharing by Co.As.It.

Principle 9: Adoption, use or disclosure of government related identifiers:

Co.As.It. will not adopt a government related identifier, such as Tax File Number or Medicare Number, for an individual when required to provide identification for individuals.

Principle 10: Quality of Personal Information

- Co.As.It. will take all reasonable steps to ensure that all personal information collected, used and disclosed is accurate, up to date and complete. However, the accuracy of that information depends to a large extent on the information that is provided.

- Employees and consumers are required to advise Co.As.It. of any changes that may affect the initial information provided.

Principle 11: Security of personal information.

Co.As.It. will protect personal information from misuse, loss, change, unauthorised access / disclosure by following the procedures outlined below;

- In the event that an employee needs to access another employee's workspace, they will seek permission from the person who normally occupies the workspace. If this is not possible or access is denied, advice will be sought from the supervisor. If urgent access is required the supervisor has the authority to access the workspace without prior consent. In the event of this occurring a witness will be present.
- Employees are not permitted to remove consumer files from the office and must ensure that filing cabinets remain locked.
- Employees will not in any way divulge, copy, release, sell, loan, alter or destroy any confidential information except as properly authorised by their professional activities.
- Employees will not misuse or negligently care for confidential information including computer passwords, access codes or any other authorisation that grants them access to confidential information. Employees will safeguard all confidential information at all times during their employment and will accept responsibility for all activities undertaken using their access code and other authorisations.
- Employees will not attempt to gain access to information that they are not authorised to see.
- Employees will report activities by any individual that they may suspect as breaches of confidentiality. Reports made about suspect activities will be held in confidence to the extent permitted by law, including the name of the individual reporting the activities.
- Any information no longer required by Co.As.It. will be destroyed and/or de-identified.

Principle 12: Access to personal information

Individuals have the right to request to view what personal information has been collected by Co.As.It.

Access to Personal Information

- We will take all reasonable steps to provide access to the personal information that we hold within a reasonable period of time in accordance with the Australian Privacy Principles.

Requests for access to the personal information we hold should be made in writing to the relevant manager.

However Co.As.It. can refuse such requests if;

- Co.As.It. reasonably believes that providing access may pose a serious threat to the life, health or safety of any individual or to public.
- Granting access would have an unreasonable impact on the privacy of other individuals.
- The request for access is frivolous or vexatious.
- The information relates to existing anticipated legal proceedings between Co.As.It and the individual and such information would not be accessible by the process of discovery in those proceedings.
- Giving access would be unlawful.
- Co.As.It. has reason to suspect that unlawful activity or misconduct of a serious nature, that relates to Co.As.It.'s functions or activities has occurred or is likely to occur;
- Denying access is required by or under Australian Law or a court/tribunal order or giving access is likely to prejudice one or more enforcement related activities conducted by an enforcement body.

Co.As.It. will notify the individual in writing of the reasons why their request to access information was refused. Co.As.It. will also advise the individual of the mechanisms available to complain about the refusal, should they not accept Co.As.It.'s decision.

Principle 13: Correction of personal information

- Co.As.It. will take every reasonable step to correct information to ensure that the information is accurate, up to date, complete, relevant and not misleading. Co.As.It. will notify any relevant third parties of any correction to personal information that was previously disclosed as deemed necessary for the delivery of services.
- Co.As.It. may refuse to correct the personal information requested by the individual. Should Co.As.It. refuse to correct such information the individual will be notified in writing outlining the reason for refusal and the mechanisms available to complain about the refusal.

Obligations under this policy and procedure extends not only for the duration of time that an employee is employed by Co.As.It but also continue indefinitely once the relationship with Co.As.It. ends.

Compliance to this policy is mandatory and failure to comply with this policy and procedure may result in disciplinary procedures or loss of employment.

Co.As.It. will:

- Incorporate this policy and procedure into induction and other training programs;
- Provide copies of Co.As.It.'s Privacy and Confidentiality Policy to consumers, employees and volunteers;
- Obtain a signed Privacy and Confidentiality Agreement.

Personal information Community Services

- Co.As.It collects and holds the personal information of customers, employees, volunteers, and contractors. 'Personal information' means information we hold about you from which your identity is either clear or can be reasonably determined. The personal information we may hold includes the following:

Consumers

- Name
- Date of birth
- Country of birth and whether you are of Aboriginal and/or Torres Strait Islander origin
- Current address
- Next of kin details
- Person responsible for customer, e.g. Power of Attorney, Enduring Power of Attorney, Guardian, Trustee, etc.
- Entitlement details including Medicare, Pension and health care fund
- Medical history
- Family medical history
- Dietary needs
- Religion
- Clinical information including assessments and monitoring charts
- Care Plans
- Progress Notes
- Financial and billing information including Income and Asset Notifications
- Accident and incident forms
- Nursing, medical and allied health information
- Photographs for marketing and community news

Employees

- Name
- Date of birth/country of birth
- Address and contact details

- Details of next of kin
- Occupation
- Employment history
- Employment Application Form
- Citizenship, passport and/or visa permit
- Medical history or fitness for work information
- Immunisation records
- Employment references
- Tax File Number
- Bank account details
- HR/personnel records including superannuation fund
- National police certificate (criminal history record check)
- Workers compensation or injury information
- Qualifications, training and competency records

Volunteers

- Name
- Date of birth/country of birth
- Address and contact details
- Details of next of kin
- National police certificate (criminal history record check)
- Drivers licence if relevant.

Contractors

- Name
- Address and contact details
- Qualifications, licenses, etc.
- Contractor Agreement
- Insurances including workers compensation, professional and public liability
- National police certificate (criminal history record check)

Breaches of Privacy

- Where a person believes that a breach of this policy or the *Privacy Act* has occurred, a written complaint should be made to the General Manager or their delegate. All complaints will be dealt with confidentially and promptly.

Notification

- Consumers, families, friends or staff who have complaints about how we have dealt with personal information may apply for an internal review.
- Applications for an internal review may concern conduct a person believes is:
    - A Breach in information protection procedure.
    - A breach in the code.
    - An inappropriate disclosure by us of personal information.
- Application for the internal review should be made in writing to the General Manager or their delegate. This application should be made within six months from

the time the applicant became aware of the alleged breach or inappropriate disclosure.

Nomination of Internal review team

- In receiving an application and conducting an internal review under the Privacy Act, we will nominate an investigation team within two weeks of receiving the complaint by the General Manager or their delegate.

Conducting the Privacy Review

- The internal review team will take the following steps in conducting the review:
- Assist the applicant as much as possible.
- Interview relevant staff, examine records and obtain any other pertinent information on the circumstances of the alleged breach.
- Seek advice from court and legal service or from Office of the Australian Information Commissioner as required.
- Determine whether a breach of the Privacy Act has occurred and, if so, what harm or damage it has caused to the applicant.
- Prepare a report and submit the finalised investigation report to the General Manager or their delegate setting out the relevant facts, the conclusions reached and recommendations for action to be taken to resolve the complaint.
- If the outcome indicates a breach of the Privacy Act has been committed, the relevant manager will contact the Australian Information Commissioner regarding the finding and the corrective actions instituted.
- The Privacy Officer will indicate outcomes to the applicants and ensure that they are aware of the Office of the Australian Information Commissioner who can investigate privacy complaints from individuals about private sector organisations and government agencies.

Completion of Internal review

- Once an application for an internal review is received, the review will be completed as soon as reasonably practicable.
- If the review is not conducted with 60 days, the applicant can seek a review by the Privacy Officer.
- Once the review is completed, the Privacy Officer may decide to:
- Take no further action on the matter
- Recommend a formal apology to the applicant
- Take appropriate remedial action
- Provide an understanding that the conduct will not occur again
- Implement measures to prevent recurrence of the conduct.

Contact Details:

- All stakeholders are encouraged to contact the management team in relation to any privacy concerns or breaches.

Related Policies

- Code of Conduct Policy and Procedure

• Disciplinary Procedures • Duty of Care Policy and Procedure • Staff Grievance Procedures	
Related Forms • Complaints Form • Privacy and Confidentiality Agreement • Schedule 1 – Australian Privacy Principles. • Consent Form (Promotional Photos/Video).	
Prepared by: Thomas Camporeale	**Date:** May 2021
Reviewed By: Maria Angelatos, Alessandra Martino	**Date:** May 2021
Approved by Co.As.It. Board on: July 2021	
To be reviewed on: July 2023	