Section 2 – Working with the Community

2.01.1 Client Privacy & Confidentiality

Why do we do things?

Communify collects and holds personal information in order to ensure that the most effective services are provided to its clients. There must be trust by the client that Communify will hold shared information confidential.

Communify is committed to ensuring the privacy and confidentiality of personal information is upheld in accordance with the Australian Privacy Principles.

Communify ensures procedures and practices comply with the 13 Australian Privacy Principles described in the Privacy Amendment (Enhancing Privacy Protection) Act 2012.

Accordingly, as a minimum, the following statements are observed in the creation or implementation of any procedures (including this procedure) or practices at Communify:

1. Open and transparent management of personal information
2. Anonymity and pseudonymity
3. Collection of solicited personal information
4. Dealing with unsolicited personal information
5. Notification of the collection of personal information
6. Use and disclosure of personal information

7. Direct marketing
8. Cross-border disclosures
9. Adoption, use or disclosure of government related identifies
10. Quality of personal information
11. Security and personal information
12. Access to personal information

What is...?

Privacy relates to many areas including the right not to be watched, listened to or reported upon without consent and not to be the focus of uninvited public attention. Privacy can be applied to clients' physical environment and possessions, physical needs, personal relationships and personal information and needs.

In Australia, privacy law generally relates to the protection of an individual's personal information. Personal information is information or an opinion about an identified individual, or an individual who is reasonably identifiable.

The boundaries and content of what is considered private differs between cultures and individuals, but shares basic common themes.

Confidentiality: A principle which states that personal information about others should not be revealed to persons not authorised to receive such information.
Personal information in the *Privacy Act* means 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.

Record means:

(a) a document

(b) a database (however kept)

(c) a photograph or other pictorial representation of a person

(d) an electronic record

Who this Policy applies to

- Board
- Employees
- Volunteers
- Sub-contractors / Brokerage services
- People who use Communify's programs, services and activities

Our Policy

Communify recognises and adheres to the Australian Privacy Principles, in accordance with the Privacy Amendment (Enhancing Privacy Protection) Act 2012, which amends the Privacy Act 1988.

These principles along with the privacy legislation set standards for Communify employees, contractors and volunteers when collecting, holding, using and disclosing private or sensitive information.

How we do things

GUIDELINES

Communify recognises the essential right of individuals to have their information administered in ways that they would reasonably expect - protected on one hand, and made accessible to them on the other.

People will be authorised to have access to this information on a *needs to know* basis i.e. they will only have access to personal information regarding clients and others that they require in order to do their job.

Communify collects and administers a range of personal information for the purposes of delivering services, such as community housing services and other support services. The type of information that Communify collects and holds relates to:

- Clients and prospective clients
- Communify employees, prospective employees and volunteers
- Contractors / Brokerage agencies
- Communify Directors
- Representatives of community, government and private agencies

Communify will have procedures relating to:

- Information collection
- Storage of information
- Disclosure of information including cross border disclosures
- Direct marketing
- Integrity of information
- Information security
- Accessing and amending information
- Archiving and destruction of information
- Complaints

If other agencies collect, store, use or disclose personal information on behalf of Communify, or if they have access to the personal information in Communify's information systems, Communify will include privacy clauses in contracts and agreements to ensure that personal information is protected from unauthorised access, use or disclosure.

PROCEDURES

Consideration of Personal Information Privacy

This procedure is to ensure that Communify manages personal information in an open and transparent way. This relates specifically to the collection, use and disclosure of private information concerning clients which is collected as part of the case management process and may include information about clients' health, families and other social relationships, personal interests, skills, behaviour patterns and financial affairs.

- The program will ensure that the personal information that it collects, uses or discloses is accurate, complete and up to date.
- All program employees will receive training in awareness of the Australian Privacy Principles.
- Employees will not proceed with client assessment and planning processes unless the client has provided consent.
- Where the client is unable to provide consent due to disability or medical condition, then consent will be obtained from their authorised representative.
- Employees will only seek information relating to clients/carers relevant to effectively providing the service. Employees operate on a 'need to know basis'. They do not seek more information about the client than is necessary to perform their roles.
- Upon initial assessment, clients are asked to sign a Client Consent form which requests agreement to the sharing of information with relevant professionals and others for the purpose of their care.
- Employees will disclose to other service providers only that information which is pertinent to the care of the client.
- Clients, through the Client Information Kit and Communify's website are provided with information about:
    - The identity of the organisation and how to contact it
    - How information about them is stored
    - Their right to access their personal information
    - Their right to request correction of their records held by Communify
- Files are recorded on all clients in standard format and notes are recorded on the Case Notes template or in specific electronic client software programs e.g. Procura, SRS.
- Progress and Case notes are written in objective terms, observing respect for the feelings and dignity of clients, the right of clients to request access to their own files, and court requirements which may subpoena client files.
- Program employees only allow access to client records to those who have a need to the information to undertake their duties.

- Program files on individual clients are kept in locked filing cabinets when not in use. When transported to Care Plan review meetings, files are placed in closed containers.
- All client related working notes that do not need to be kept permanently are shredded.
- Notes recorded on the computer are protected by a password and are subject to the same requirements as written notes.

Communify will utilise the following strategies to ensure that privacy and confidentiality requirements are met with respect to clients:

- Communify will only collect information pertaining to clients' support and referral needs.
- Information will be collected in a fair and non-intrusive way in a private environment.
- Clients are informed regarding the purpose of collecting information and of their rights pertaining to privacy and confidentiality, including the processes for accessing information held about themselves and how to make a complaint regarding alleged breaches of confidentiality or privacy.
- Clients may view Communify's Privacy and Confidentiality Policy on the website or request a copy by contacting Reception.
- Confidential information will be stored in lockable filing cabinets (if paper-based) or on a password protected computer or Server (if electronic). Filing cabinets will be locked at all times when not being accessed.
- Paperwork containing client or other confidential information will not be kept on desks if there are no employees present to safeguard confidentiality.
- Care will be taken when holding discussions with clients that they cannot be overheard by people not involved in working with them. This includes phone conversations in shared offices.
- Clients will be informed during initial contact of the details of the confidentiality policy, in particular their attention will be directed to the confidentiality limitation conditions.
- Awareness of Communify's privacy policy and procedure will form part of the orientation process of all Program employees.
- Relevant employees will organise home visits with clients/carers at times that are suitable to both parties.
- Relevant employees will ensure that the clients' physical needs are attended to during activities in a way, which respects the comfort and dignity of the person. This includes personal care, incontinence aids and clothing changes.
- Employees will ensure that the private property of clients is treated with respect.

Anonymity & Pseudonym

Where it is lawful and practicable, individuals will have the option of not identifying themselves when entering into transactions with Communify.

Clients may also request to use a pseudonym and may do so where able, when receiving services.

Information Collection

Communify needs to collect information relevant to providing a service which are governed by legislation, if a client, applicant, owner or contractor does not wish to provide personal information, then Communify may not be able to provide a service or use their services.

Communify collects information from clients and prospective clients in order to develop an appropriate response to their needs. Communify collects information relating to clients or prospective clients via third parties e.g. referrals from other agencies, family members / carers and from prospective client themselves

The personal information Communify collects from clients or prospective clients may include:

- Name and contact details
- Medical / disability information
- Representative, advocate, case worker, support worker details
- Guardian or administrator details
- Household members details
- Cultural background and preferred language
- Financial information
- Citizenship / residency status
- Previous name(s)
- Location and type of assistance sought
- Any pets they might have (for tenancy purposes)
- Transport
- Emergency contact details
- Progress notes

Communify employees may use personal information for determining eligibility, possible referrals and case management purposes.

As Communify does not manage or store personal information that is not relevant to its delivery of services, the following actions may be taken if a document is received that contains unnecessary information:

- Note the relevant information and return the document
- Blank out the irrelevant parts of the document before storing, or
- Note that the document has been sighted and return it.

Communify will provide a private place for face-to-face interviews at which personal information is collected. Employees will ensure that face to face and telephone conversations with applicants and clients are conducted in a way in which personal information may not be overheard.

Contractors and other services (i.e. brokerage agencies) are provided with client information relevant to undertaking repairs and maintenance on the property. Communify will provide contractors with:

- Property address
- First name of client
- Contact number

In conversations with the Communify employee about their needs, client's consent to release information is confirmed.

Limitations to confidentiality

The employee will explain the limited confidentiality conditions including where:

1. Information may be shared at internal case conference meetings. This will be on a *needs to know* basis i.e. only personal information relevant to the provision of services to a client will be only shared with staff members who require that information to undertake their duties.
2. Non-identifying information will be shared with senior staff and across agencies involved in coordinated community responses to systemic issues
3. Communify believes that:
    - The safety of a client, their children, the staff member, other clients or any other person is at risk
    - There is suspected child abuse or neglect
    - A serious criminal offence has occurred or is likely to occur
4. Communify believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to an individual's life, health or safety or a serious threat to public health or public safety
5. Communify has reason to suspect unlawful activity and use or disclose the personal information as part of an investigation of the matter or in reporting our concerns to relevant persons or authorities
6. Communify employees reasonably believe that the use or disclosure is reasonably necessary to allow an enforcement body to enforce laws, prevent seriously improper conduct or prepare or conduct legal proceedings
7. The use or disclosure is otherwise required or authorised by law.
8. Employees are authorised to share information with an external supervisor for the purposes of supervision and debriefing.

In these cases the employee will follow the relevant policy e.g. Child Protection and Risk Management, Elder Abuse, etc.

Consent / Information Disclosure

Communify employees will ensure that clients are informed about how their personal information will be used. This should include an understanding of:

- Who will access information
- The reason why information is collected
- Whether collection of information is voluntary or mandatory
- How information will be used
- The authorised personnel who have access to it
- Disclosure of information in certain situations.

Communify will use personal information only for the purpose for which it was collected and disclose personal information only if the individual or their guardian is reasonably aware of or has consented to that disclosure. The exceptions to this are:

- Where the safety of the client, their children, an employee or other persons is at imminent risk
- Where there is suspected child abuse or neglect, or
- Where records are subpoenaed or required by law.

There may be instances where clients are not in a position to give consent. In these situations, employees will make use of next of kin, carers or other formal or informal advocates to seek informed consent.

Non-identifying information may be shared across agencies involved in coordinated responses or other partnership arrangements. When this occurs, processes involved will be consistent with the Australian Privacy Principles.

If access to records is authorised or required by statute, prior to any release of this type of information, employees must advise the Chief Executive Officer.

Communify will support the rights of all clients to obtain access to copies of information held by them regarding that client.

When first becoming a client of Communify, clients will be informed, as a matter of routine, about their rights of access to their own records.

Access to client information for use by approved research projects will only occur with the client's consent. Where possible, a consent form will be completed by the client or carer/guardian.

Clients will be assured that their personal information will be protected regardless of the form in which the information is held (e.g., hard or electronic copies).

Client records compiled and kept by Communify are the property of Communify.

Communify will release information concerning clients to those clients and others only upon receipt of a request or authority signed by the client.

Disclosure to any third party is not permitted, except when required by law. Disclosure may be required by law in the following circumstances:

- Pursuant to a court order
- Pursuant to a writ of non-party discovery
- Pursuant to an order of a coroner or some other tribunal created by statute
- Pursuant to other provision contained in statutes
- Pursuant to a police search warrant
- Statistical information from minimum data sets as required by government.

All instances of disclosure to a third party will be noted on the appropriate record (progress notes for clients, employee file for employees, etc.). Information to be noted will include:

- Name of the person who disclosed the information
- If written or verbal consent was obtained
- Date and purpose of the disclosure
- Name of the person and agency to whom the information was disclosed.

Some documents may be privileged and as such do not have to be disclosed. Privileged documents can include those prepared solely for the purpose of obtaining legal advice or in anticipation of or during court proceedings.

Disclosure may also be desirable in the following situations:

- Where the interest of the client requires disclosure such as case conferencing with other health professionals involved in the client's care: and/or where there is a duty to the public to disclose such as the provision of information to the police to assist in enquiries.
- In these cases disclosure must not be made unless the client's consent (in writing) is obtained.

Adoption, use or disclosure of Government related identifies

Communify is prohibited from adopting, using or disclosing a government related identifier unless an exception applies (please see Australian Privacy Principles for further information relating to exceptions).

Integrity of Personal Information

To ensure that personal information collected is kept accurate up to date and complete Communify employees will

- Regularly ask client during contact if details on file correct
- Scheduled reviews includes review of personal information

Right to access and / or amend records

(a) Accessing information

- Clients have a right to read any personal information kept about them.

- Request from clients (or authorised representatives) to access information will be referred to the relevant senior employee who will ensure that assistance is provided to the client to access their information within 10 working days of the request being received.
- A client does not need to provide a reason for requesting access.
- A fee will not be charged for lodging a request for access.
- An employee will be available to the client to explain terminology or provide assistance.
- If access to records is requested, workers are to inform clients that they may read copies of official documents or employee notes that relate to them on the premises but not take them home.
- Photocopies of documents will be provided within resource limitations.
- Communify is the owner and controller of all client records. No records may be removed from the premises without specific written approval by the Chief Executive Officer, in consultation with legal advisors (if required).

(b) Refusing a request to access personal information

A request by a client to access information held about them may be refused, if

- Communify reasonably believes that giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety; or
- Giving access would have an unreasonable impact on the privacy of other individuals; or
- The request for access is frivolous or vexatious; or
- The information relates to existing or anticipated legal proceedings between Communify and the individual, and would not be accessible by the process of discovery in those proceedings; or
- Giving access would reveal the intentions of Communify in relation to negotiations with the individual in such a way as to prejudice those negotiations; or
- Giving access would be unlawful; or
- Denying access is required or authorised by or under an Australian law or a court/tribunal order; or
- Both of the following apply:
    - Communify has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to Communify's functions or activities has been, is being or may be engaged in; and
    - Giving access would be likely to prejudice the taking of appropriate action in relation to the matter; or
- Giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or

- Giving access would reveal evaluative information generated within Communify in connection with a commercially sensitive decision-making process.

The decision to refuse a request can be made, in the first instance, by the relevant Program Manager. If the client wishes to appeal this decision they can use Communify's Client Complaint policy.

(c) Changing information

If a client believes that the personal information held about them is inaccurate, incomplete or not up-to-date, the client may request an amendment.

If a client makes a straightforward request for an amendment, for example to correct a name or address, Communify will usually make the change, subject to confirming the new information.

In other circumstances, for example if a client queries the accuracy of case management notes, Communify will generally amend the client's record by attaching comments to the record noting the correct information or a statement that the client claims that the information is not accurate, complete or up-to-date. However, in no circumstances will the original entry be deleted.

Archiving and destruction of information

Archived information is securely destroyed after the following time periods:

Document type	Length held before destroyed
Employees records:	Seven (7) years
Employment applications	Successful applications (see above) Unsuccessful applications: 6 months
Client records	Seven (7) years
Financial records	Seven years
General administrative records	Seven (7) years
Minutes of Board meetings	Indefinitely

When destroying records after the expiry date of the storage period, it must be done in such a way that the records are completely destroyed in a secure manner by shredding or incineration (in accordance with local authority by-laws).

Deletion of electronic records must conform to relevant Australian Standards.

Cross-border disclosures and overseas recipients

An 'overseas recipient' is a person who receives personal information from an Australian organisation and is:

- Not in Australia or an external Territory
- Not the organisation disclosing the personal information, and
- Not the individual to whom the personal information relates.

Communify's data is all backed up within Australia. Any cloud based applications and associated data reside within Australia. Care should be taken, however in sending of personal information to web-based email addresses such as Yahoo, Gmail and Hotmail as this information could be stored outside of Australia, in countries which do not have privacy legislation comparable to Australia's. Clients and other Communify stakeholders will be advised of the possibility of information going to such countries.

Communify will take all steps that are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian Privacy Principles.

Privacy and confidentiality training

Induction sessions run for new Board Directors and employees outline Communify' s legal and professional obligations with respect to privacy and confidentiality and training is provided in strategies utilised to ensure compliance.

Client information and the Communify Board

Communify clients will not be identified by name in reports to the Board.

All new Board Directors are made aware of their responsibilities regarding confidentiality as part of their induction and written guidelines and information kits given to new and potential members.

Breaches of confidentiality

All employees, volunteers and contractors will sign a Confidentiality Agreement at the commencement of their involvement with Communify. Any breach of this Agreement will be investigated and may result in dismiss or termination of contract.

Promotion of Client Activities

Communify may use personal information such as phone number, postal address or email to contact clients of scheduled activities. Clients may advise Communify in writing if they do not wish to be contacted in this way.

Direct Marketing

Communify will not disclose personal information to a third party for direct marketing.

Complaints regarding non-compliance with this policy

Clients and others who believe that Communify has not complied with this policy may use Communify's Client and Community Complaints policy to lodge a complaint.

How Policy change happens

This policy will be reviewed every 2 years or following legislative changes. Data that can assist in this review process may be gathered from:

- Internal audits
- Client feedback / complaints
- Employee feedback / complaints
- Board feedback / complaints

Our Obligations

This policy relates to the following Practice Standards and legislation:

- **Human Services Quality Standards** - Standard 1 Governance and Management; and Standard 4 Safety, Well-being and Rights
- **Home Care Standards** – Standard 3 Service User Rights and Responsibilities; EO3.2 Privacy and Confidentiality
- **National Regulatory Code (Community Housing)**: Standard 4 Governance
- Australian Mental Health Standards - 1.8, 1.14, 7.7.
- Commonwealth *Privacy Act 1988*
- Commonwealth *Privacy Amendment (Private Sector) Act 2000*
- Privacy Fact Sheet 17 - Australian Privacy Principles

Relevant Forms and/or Documents

- Disclosure of Information form
- Client/Service User Consent form
- Client Handbook
- Compliment, Suggestion & Complaint Form
- Client/service user survey

Related Policies and Procedures

- 2.10 Elder Abuse
- 2.11 Child Protection and Risk Management
- 2.12 Client and Community Complaints
- 2.13 Feedback Processes

Approval Date:	March 2008
Date Amended/Reviewed:	March 2016, February 2017
Date to be Reviewed:	February 2019