Supporting our community on all sides

P O L I C Y

2 Working with the Community

2.00 Client Privacy Policy

Policy 2.00 – Client Privacy Policy

Why we do things

Communify collects and handles personal information in accordance with relevant laws and to ensure the most effective services are provided to its clients. Communify is responsible for implementing systems and processes to ensure a client's personal information is confidential.

Communify is bound by the Privacy Act 1988 (Cth) and will protect all information in accordance with the thirteen Australian Privacy Principles set out in Schedule 1 of the Privacy Amendment (Enhancing Privacy Protection) Act 2012. These principles govern how Communify can collect, use, store and disclose personal information, how individuals may access and correct personal information held about them, and ensuring the quality and security of personal information.

Communify will only collect necessary information about people that will enable the provision of requested supports and services. Information will be collected from individuals, and with their consent, from other stakeholders such as family members, carers, other support services and government agencies. Communify keeps people informed about the types of information collected and how this information will be used.

Communify ensures breaches are reported in accordance with the Privacy Amendment (Notifiable Data Breaches) Act 2017 as outlined in the Client Information Management Policy.

This Privacy Policy explains how Communify Queensland Ltd collects, uses and handles personal information of clients.

Definitions

Personal Information: In this Privacy Policy, personal information means information (including images) or an opinion about an identified individual, or an individual who is reasonably identifiable. It includes information or opinion:

- Whether the information or opinion is true; and
- Whether the information or opinion is recorded in a material form or not.

Personal information includes (but is not limited to) information such as:

- Name, date and place of birth
- Race or ethnicity
- Financial/banking details
- Health/diagnostic information
- Employment details
- Photograph (including CCTV footage)
- Signature
- Uniquely identifying number – e.g., driver license number, tax file number
- Details of services requested or obtained
- Unique physical characteristics – e.g., tattoo, birthmark

Personal information includes information, which we request and information that is given to us, which we have not requested.

Health information – Any information or an opinion about the physical, mental, or psychological health or ability (at any time) of an individual.

Privacy: Under the Commonwealth Privacy Act, privacy relates to personal information. For Communify, privacy also relates to physical privacy that is, having a private space for oneself, or to speak about service or other issues.

Information Privacy: Refers to the control of the collection, use, disclosure and disposal of information and the individual's right to control how their personal information is handled.

Confidentiality: Is the protection of personal information and means keeping someone's information between you and them, and not telling anyone else unless they have given you informed consent to do so.

Records: Includes documents, databases (however kept), photographs or other pictorial representations of a person and electronic records.

Who this policy applies to

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

Our policy

Communify protects and upholds the privacy and confidentiality of clients and staff. To protect and uphold privacy we:

- Have processes in place, so no personal information is collected, stored, used or shared with anyone, purposefully or by omission, unless the client provides informed consent or we are required by law to do so.
- Only collect the information needed to perform services.
- Store all data securely as per legislation.

To maintain confidentiality, we:

- Uphold all legal and ethical obligations concerning handling confidential information.
- Provide information to clients and staff about their rights regarding confidentiality and the processes used to protect these rights, and where any limits to confidentiality exist.
- Avoid inappropriate verbal and written disclosure of information about clients and staff within and outside of the organisation.
- Only share verbal and written information about a client with agencies and individuals external to Communify with the written consent of the client, unless the circumstances are such that limits to confidentiality apply.

- Take all reasonable steps to protect all information held (including personal information) from misuse, loss, unauthorised access, modification, or disclosure.

How we do things

Communify collect personal information from a person when they:

- Submit a query or request to Communify
- Are referred to Communify by a third party (with consent where required)
- Participate in programs or events that Communify run or support
- Receive Communify products or services
- Respond to a survey or fill in one of our forms

Types of personal information Communify collect include:

- Identifying information, such as name and date of birth
- Details of services that we provide to a client
- Information about how a client uses the services we provide
- Information about how a client accesses other services
- Records of our interactions with a client
- Contact information, such as address, email and phone number
- Financial information, such as credit card, bank account or other payment details
- Government-issued identifiers - such as health service providers' practitioner numbers
- Usernames and passwords that a person creates when registering for an account with us
- Social media profile information that you make available to Communify or to the public
- Information about health
- Photographs and video recordings.

Informed consent in the collection of personal information:

Communify will only collect personal information about a client with their permission, except where the law requires or allows. Information will be collected from the client, and, with their consent, from other stakeholders such as family members, carers, other support services and government agencies.

Clients are informed during initial contact of the details of the Client Privacy Policy. Communify will keep the client informed about the types of information collected and how it will be used.

Communify tells its clients:

- The identity of the organisation and how to contact it
- What information is collected
- Why it is collected
- How we use their information
- When information may need to be released or disclosed
- Their right to decline to provide information
- When we can release their information without their consent
- Their right to make a complaint about privacy and confidentiality at any time
- How to make a complaint regarding alleged breaches of confidentiality or privacy
- How information about them is stored
- Who will access their information

- Their right to access their personal information
- Their right to request correction of their records held by Communify
- Information is kept up-to-date and accurate
- How to access Communify's Privacy Policy on the website or request a hard copy.

When asking for consent, Communify must explain the reason for the request and be as specific as possible, and will not ask for broader consent than is necessary. When consent is provided at a particular time and for specific circumstances, Communify will not assume that the consent continues indefinitely. The client will be informed of the period for which the consent will be valid and that they can withdraw their consent at any time.

Service delivery does not proceed unless the client has signed a Privacy Collection Notice and Consent Form. This includes documenting consent to share information with relevant external agencies for the purpose of coordinated service delivery. Where the client is unable to sign a Privacy Collection Notice and Consent Form due to disability or other condition, consent is obtained from their authorised representative.

How personal information is collected by Communify:
We collect personal information in several ways. These are face-to-face, over the phone, by email, over the internet (including social media platforms); and in writing. Information is collected in a fair and non-intrusive way in a private environment. Clients' physical needs are attended to during activities in a way that respects the comfort and dignity of the person.

Only information relating to effectively providing service is collected. Employees operate on a 'need to know' basis. Employees do not seek more information about the client than is necessary to perform their roles. Communify may also collect personal information from our service providers whom we engage to provide services on our behalf, where relevant consent exists. Employees only disclose to other service providers information that is pertinent to the interest of the client.

Communify may collect personal information by tracking use of our websites and mobile applications (in which case Communify may also collect information about an individual's IP address, location or activity). This information helps us to keep connected with a person through understanding use of our website. The information collected may include information to enable us to personalise a person's experience on our website and to enable us to statistically monitor how they are using our website.

Communify may also use this information to conduct marketing and promotional efforts, to provide information to a person's browser that we think may be of interest to them, to determine the popularity of certain content.

Integrity of Personal Information
To ensure that personal information collected is kept accurate, up to date and complete, Communify employees will:

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

Purposes for which we collect and use personal information:

When Communify collect personal information, we will provide the person with more information about the reason for the collection. Communify may also tell them more about any other specific matters that are relevant to collecting that information. If they have agreed, we collect and use personal information for one or more of several purposes. These will depend upon what is relevant to their situation to enable us to:

- Determine eligibility
- Establish the client's service requirements
- Provide support through our various community programs
- Provide possible referrals and case management processes
- Manage our relationship with the person, including confirming their identity, responding to any queries or requests and by contacting them for follow-up purposes
- Contact the client or their authorised representative in an urgent situation
- Provide products and services
- Work together with other key people and agencies who provide or may provide supports and services to the client
- Raise funds
- Analyse use of our products and services, and carry out quality assurance activities, including through working with third parties
- Provide education and training, both internally and externally
- Keep clients informed of our activities, including through sending out newsletters and electronic communications
- To report identified statistics to our funding partners about services that the client has been provided
- Manage and develop our business and operational processes and systems
- Manage and resolve any legal or commercial complaints or issues
- Comply with our legal obligations
- To report internally and conduct research and program evaluations. Information used for these purposes will not contain any details that identify the client

We may also use and disclose personal information in accordance with a person's requests or instructions.

People to whom Communify disclose personal information:
The personal information gathered is only accessible to authorised Communify employees. Employees will only access the records of those whose information is needed to undertake their duties. Communify will not use or disclose any information about a client for other purposes without consent, unless the law or safety concerns requires us to do so. For example, we are concerned about your or another person's health or safety.

Where a person has consented, Communify may share personal information with some other people. This will depend upon what is relevant to their situation. Communify will ensure that informed consent is obtained around the collecting and sharing of their personal information. Communify will provide the person with more information about the reasons for the information to be shared.

If a person has agreed, the other people with whom Communify may share personal information, depending upon their situation, could be amongst those listed here:

- Our staff, contractors and volunteers, on a 'need-to-know' basis
- Our business partners, agents, professional advisors and service providers (including health service providers, translators, interpreters and other third parties we work with or engage, to provide our services).
- Client representatives and advisers
- Government agencies, such as those who we receive funding from
- Universities and research organisations
- Payment system operators and financial institutions
- Other parties as authorised or required by law

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.

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.

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

Communify may need to disclose personal information to a third party located overseas, for a purpose set out in this Privacy Policy. In this case, Communify will only do so to the extent necessary. Communify will also take reasonable steps to ensure that the third party handles personal information in accordance with Australian privacy laws.

Communify may also disclose personal information to overseas organisations where a client tells Communify to do so or expresses consent to us doing so. In such cases, it may not be possible or appropriate for Communify to take the steps set out above in relation to the management of the information. Communify will tell the client about this at the time.

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).

Limitations of confidentiality

Individuals will be made aware of confidentiality conditions including where:

- Information may be shared at internal case conference meetings. This will be on a *need-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.
- Non-identifying information will be shared with senior staff and across agencies involved in coordinated community responses to systemic issues.
- 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
- 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
- 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
- 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
- The use or disclosure is otherwise required or authorised by law
- Employees are authorised to share information with an external supervisor for the purposes of supervision and debriefing

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.

Anonymity and pseudonym
Where it is lawful and practicable, individuals 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.

Right to decline to provide information:
A person may choose not to agree to provide the personal information Communify request. If this choice is made, then Communify may not be able to provide that person with some or all of our support, products, services, or opportunities or Communify may not be able to engage with that person or respond to their queries or requests.

By providing personal information to Communify, the client confirms that they have agreed to Communify collecting, using and disclosing their personal information in accordance with this Privacy Policy.
Communify may collect sensitive information about a client, such as health information. When we do so, we will seek that person's consent to the collection, use and disclosure of that information at the time of collection.

Storage and security of personal information:
Communify stores the personal information that we collect in secure access-controlled client or document management software systems. Some of these systems may be held on our behalf by third party hosting providers such as Microsoft or Amazon.

We may also keep hard copy records of personal information in physical storage facilities. Hard copies of personal information must be stored in locked filing cabinets. When transported, files are placed in closed containers. All client related working notes that do not need to be kept permanently are shredded.

Communify ensure that care is 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.

Communify use physical and information security processes to protect the confidentiality and security of the information that we hold. When the personal information is no longer needed, the records are securely managed in accordance with relevant State Archives processes. The archiving and destruction of information is outlined in this policy.

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.

Keeping information safe and preventing data breaches — obligations under the Privacy Act
Communify has a number of strategies and processes to protect the personal information we hold from misuse, interference and loss.

Any data breaches will be reported in accordance with the Privacy Amendment (Notifiable Data Breaches) Act 2017.

Archiving and destruction of information

Archived information is securely destroyed after the following minimum time periods:

Document type	Minimum length held before destroyed
Employees records	Seven (7) years
Employment applications	Successful applications (see above) Unsuccessful applications: 6 months
Client records	Seven (7) years
Client records (Childcare Providers)	Until the child is twenty-five (25) years old
Client records relating to child sexual abuse that has, or is alleged to have occurred (services that engage in child-related work)	Forty-five (45) years
Financial records	Seven (7) 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 are 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 that do not have privacy legislation comparable to Australia's legislation. Clients and other Communify stakeholders will be advised of the possibility of information going to such countries.

Access and correction:

At any time, a client can lodge a request in person, by email, phone or letter if:

- They would like to access their information
- Believe that their information held by Communify is inaccurate or not up to date, and would like to correct some aspect

Accessing information:

- Clients have a right to read any personal information kept about them
- Communify will release information concerning clients to those clients and others only upon receipt of a request or authority signed by the client
- 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)

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
- Giving 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 or anticipated legal proceedings between Communify and the individual, and would not be accessible by the process of discovery in those proceedings
- Giving access would reveal the intentions of Communify in relation to negotiations with the individual in such a way as to prejudice those negotiations
- Giving access would be unlawful
- Denying access is required or authorised by or under an Australian law or a court/tribunal order
- 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
    - Giving access would be likely to prejudice the taking of appropriate action in relation to the matter
- Giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body
- 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 Senior Manager. Where access is denied, Communify must provide written advice as to the reasons for denial of access and/or give the client access to those parts of the record/file that are not exempt. If the client wishes to appeal the decision, they can use Communify's Client and Community Complaints policy.

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

Queries and complaints:

Communify aim to always meet the highest standards to safeguard privacy. A person may like to discuss any information contained in this Client Privacy Policy or lodge a complaint about how their personal information is collected or used, or regarding the outcome of a request to access or correct their information. If so, Communify can be contacted using the contact details below. Communify will make a record of the complaint or query and will deal with the matter as soon as we can. Staff must refer to the Client and Community Complaint policy.

Contact Details

Communify Queensland Ltd
180 Jubilee Terrace, Bardon QLD 4065
Phone: (07) 3510 2700
Email: admin@communify.org.au

If Communify have not tended to a complaint or query within a reasonable time or if the person feels that a complaint has not been resolved to their satisfaction, they are entitled under the Privacy Act to make a complaint to the Office of the Australian Information Commissioner. You can contact that office:

- by phone on 1300 363 992
- Teletypewriter (TTY) users' phone 133 677, then ask for 1300 363 992
- Speak and Listen users' phone 1300 555 727, then ask for 1300 363 992
- Internet relay users connect to the National Relay Service, then ask for 1300 363 992.

Ongoing training and Support

- 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
- All employees receive information about the Australian Privacy Principles
- Raising staff awareness of privacy and confidentiality through induction and team meetings
- 2.00 Privacy Policy located on Communicate
- 2.00 Privacy Policy is available on the Communify website

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 are 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 dismissal 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 if consent has been provided to do so.

Direct Marketing

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

How policy change happens

This policy will be reviewed every two years or following legislative changes. Information that can inform this review includes:

- Board Director feedback
- Employee feedback
- Client feedback/complaints
- Changes in legislation
- Internal Audits

Our obligations

This policy relates to the following Practice Standards and legislation:

- Human Services Quality Standards
- Aged Care Quality Standards
- NDIS Practice Standards
- National Regulatory Code (Community Housing): Standard 4 Governance
- National Quality Standards (Childcare)
- Commonwealth *Privacy Act 1988*
- *Information Privacy Act 2009* (Qld)
- Human Rights Act 2019
- Right to Information Act 2009 (Qld)
- Privacy Amendment (*Enhancing Privacy Protection) Act 2012*
- Privacy Amendment *(Notifiable Data Breaches) Act 2017*
- Commonwealth *Privacy Amendment (Private Sector) Act 2000*
- Privacy Fact Sheet 17 - Australian Privacy Principles
- Information Sharing Guidelines (Section 5A) of the Domestic and Family Violence Act 2012
- Section 159C of the Child Protection Act 1999
- Disability Services Act 2006

Relevant forms and/or documents

- Client Handbook
- Client/service user survey
- Communify Privacy Collection Notice

- Communify Risk Management Register
- Compliment, Suggestion and Complaint Form
- Compliments, Suggestions and Complaints Register
- Media Consent Form
- Service Consent Forms

Related policies and procedures

- 2.01.1 Client Information Management
- 2.10 Elder Abuse
- 2.11 Child Protection and Risk Management
- 2.12 Client and Community Complaints
- 2.13 Feedback Processes
- 3.09 Regulatory Compliance
- 3.12 Information Technology and Cyber Security
- 6.15 Closed Circuit Television (CCTV)

Approval date	October 2019
Date last amended/reviewed	May 2022, May 2024
Date to be reviewed	May 2026