

## PRIVACY POLICY

### Source Documents

- *Privacy Amendment Act (2000)*
- *QLD Disability Services Act (2006)*
- *QLD Disability Services Regulations (2006)*
- *QLD Human Services Quality Framework*
- *QLD Child Protection Act (1999)*
- *QLD Child Protection Regulations (2000)*
- RCS Complaints and Feedback Policy
- RCS Continuous Improvement Policy

### 1. PURPOSE:

This policy has been designed with recognition that Real Community Services must adhere to the National Privacy Principles and the Privacy Amendment (Private Sector) Act 2000. These principles and the privacy legislation set standards that must be met when collecting, holding, using and the disclosure of private or sensitive information.

### 2. SCOPE:

This policy applies to employees and volunteers. All levels of management are committed to the implementation of this policy and are responsible for taking appropriate disciplinary action where required.

### 3. DEFINITIONS:

For the purposes of this policy, the following definitions apply:

**Privacy** refers to a person - that is, about his or her body, support needs, family and friends, relationships, lifestyle, home, workplace, belongings, and finances.

**Confidentiality** refers to information of a person or organization (written, spoken and observed) - that is about conversations, file, reports, programs, activities.

**Dignity** refers to treating a person or referring to a service, organisation with respect at all times.

### 4. POLICY:

At all times Real Community Services recognises and respects each person's right to privacy and dignity by:

- Being treated with respect and with consideration to cultural and personal beliefs
- Ensuring that information is protected from access and use by unauthorised persons.

### 5. PROCEDURES:

#### 5.1. Collection of Disclosure

## PRIVACY POLICY

- Information will only be collected that is necessary to perform legitimate functions or activities and will only be collected by fair and lawful measures. This includes:
  - Information on organisations, clients and their families that is directly relevant to service delivery
  - Information about Real Community Services employees such as contact details, tax file and bank account details, skills, qualifications and experience and any other relevant information.
- No information is collected about an individual without their written or implied consent (or the written consent of person responsible or guardian) unless disclosure is required by law.

### 5.2. Information Security

- Hard copy confidential information is stored in key lockable filing cabinets. Filing cabinet keys are only accessible to persons with authority to access the particular information contained within each filing cabinet
- Electronic information is stored on a password secured computer network. Password access to Real Community Services network drive is provided to office-based staff only.
- Hard copies of confidential information that is intended to be used at a in secure location or Electronic copies of confidential information that have been stored outside of the secure network and or emailed, Should contain a some form of privacy Disclaimer.
- Personal or confidential information that is no longer required by Real Community Services (in consultation with applicable taxation / wages and medical legislation), is de-identified or destroyed via secure destruction methods

### 5.4. Access to Your Information

- You have a right to see and have a copy of personal and or sensitive information about you that we may hold [subject to Principle 6 – Access and Correction, in the National Privacy Principles in the *Privacy Amendment (Private Sector) Act 2000*].
- Should a person request access to information, the Service Manager or representative will coordinate assessment of the requested information and determine if access can be made in full, in part or if it must be denied.
- The Service Manager or representative will consider third party requirements and exceptional circumstances when considering this request. Access to personal information may be denied because:

## PRIVACY POLICY

- in the case of personal information other than health information—providing access would pose a serious and imminent threat to the life or health of any individual / organisation
- in the case of health information — providing access would pose a serious threat to the life or health of any individual;
- The applicant for the release of personal information on a consumer is not an authorised representative of the consumer
- Providing access would have unreasonable impact upon privacy of other individuals
- the request is frivolous or vexatious
- the information relates to existing or anticipated legal proceedings between the organisation and the individual, and the information would not be accessible by the process of discovery in those proceedings;
- providing access would reveal the intentions of the organisation in relation to negotiations with the individual in such a way as to prejudice those negotiations
- Providing access to the information may put the requester or another person at risk of harm, or if it would be unlawful to release the information (e.g. if the information would lead to identifying someone reporting harm under the Child Protection Act 1999). In these cases, access may need to be denied unless some information or names of third parties can be removed.
- Providing access would be unlawful
- denying access is required or authorised by law;
- providing access would be likely to prejudice:
- Where restriction of information is indicated, the Service Manager will take advice from the Managing Director concerning release of information.
- Within 14 days of receipt of request, the Service Manager or representative will advise the requester in writing, or the most appropriate format, of the decision.
- The Service Manager or representative will ensure that the person has access to a private room and a third party support in attendance if requested (at no cost to RCS) in order to view the approved information.

## EVALUATION

Review Date:	01 December 2015
Author:	T. Green (Director)
Implemented:	01 December 2015
Review Cycle:	12 Months
Next Review Due:	01 December 2016