COMMUNITY GATEWAY

Privacy and Confidentiality Policy

Policy Statement:

Northern Rivers Community Gateway (the Community Gateway) places great value on earning and maintaining the trust of clients, employees and others whose private, personal or sensitive data or other confidential information is shared with us. In today's community services environment, the privacy protection of information is important for both electronic records and paper-based records.

Personal information collected by staff is handled in accordance with legislation, organisational policy and code of conduct, which affirm commitment to the protection of confidential data including, as appropriate, the protection of personal data under the Australian Privacy Principles.

The Community Gateway affirms its commitment to the privacy of the information provided by our clients and respects the privacy of staff, other workplace participants and individuals.

Purpose:

The Community Gateway is committed to ensuring all Board members, management, staff and others involved in the operation of the organisation comply with their obligations under privacy legislation. This document outlines how we manage personal information and adhere to privacy laws both in intent and procedure.

Definitions:

Consent means 'express consent or implied consent'. The four key elements of consent are:

- you are adequately informed before giving consent
- you give consent voluntarily
- consent is current and specific, and
- you have the capacity to understand and communicate your consent.

'Personal data' is information or an opinion that identifies or could reasonably identify an individual, directly or indirectly. Examples include name, address, bank details, photos, videos, information about personal preferences and opinions, occupation, physical, physiological, mental, economic, cultural or social identity - any information, recorded or unrecorded, where an individual may be reasonably identifiable.

Under privacy law, personal information includes 'sensitive information' – racial or ethnic origin, political opinion or association, religious belief or affiliation, philosophical belief, professional, trade or union membership, sexual preference or practice, criminal record; and

'Health information' – including physical or mental health, disability, preferences, use of and future provision of service, bodily donations and genetics, medical appointments, notes reports and results, pharmaceutical purchases and any other personal information collected to provide a health service (afforded higher level of protection under privacy laws)

Spent convictions (old, minor convictions), tax file numbers, surveillance information and credit history are also protected confidential information under privacy law.

Related Legislation and Policy:

- Privacy Act 1988 (Commonwealth) which includes the Australian Privacy Principles, Freedom of Information Act 1982, Australian Information Commissioner Act 2010, Community Welfare Act 1987, Privacy and Personal Information Protection Act 1998 (NSW), Health Records and Information Privacy Act 2002 (NSW), Education and Care Services National Regulations, Fair Work Act 2009, Chapter 16A of the Children and Young Persons (Care and Protection) Act 1998, Australian Charities and Not-for-profits Commission Governance Standards
- Code of Conduct, Information Management Policy, Data Management and Protection Policy, Recordkeeping and Archive and Storage Policy, Data Breach Response Plan, Staff Social Media Policy, Reporting Requirements About Children Procedure, Mandatory Reporting Flowchart, Reportable Conduct of a Staff Member, External Complaint Policy, Photo, video, story consent form, Data Exchange Protocols, SHS Data Collection Manual, NILS Manual, Chapter 16A Factsheets, Managing People's Information and Data (ACNC), Appendix: Permitted Situations Quick Reference.

Application:

This policy applies to all employees, volunteers, Board and representatives.

Guiding principles:

Our *Purpose and Practice Framework* details our model of informed consent: we are transparent about why and how we collect information, how it is stored, and how it is used by us to inform organisation and service decisions.

We follow the *Australian Privacy Principles* maintained by Office of the Australian Information Commissioner and are committed to:

- be ethical, respectful, truthful and in no way misleading;
- provide timely and appropriate notice about data practices including when and why we collect your personal information, what we will do with it, and how you can gain access to and correct this information we hold; and
- collect, store, hold, use or disclose your personal data for the specific, legitimate business purposes for which it was collected.

Information we collect and hold:

We may collect personal, sensitive and health information from you but only as reasonably necessary to provide the best possible services and programs and fulfil our funding obligations.

We will always advise you and gain your consent to use your personal information for any secondary purpose.

Reasons why we collect, hold, use and disclose your personal information

There are many reasons why we collect and hold personal information, including to:

- assess the need for and provide the highest standard of service possible
- meet obligations under relevant legislation
- ensure health, safety and welfare of clients, volunteers and staff
- conduct and improve business operations and programs.

How we collect personal information

We collect personal information directly from you and sometimes from a third party (such as a carer or authorised representative) usually with your consent.

Where this is sensitive or health information we must ask for your consent, unless an exception applies. Even in these circumstances we will notify you we have collected your personal information.

We may receive your personal information in person or in writing, by phone, or electronically.

We will always collect your personal information in a lawful and fair way and if practical, collect this directly from you and not a third party. If we receive information from a third party (such as a referrer) we will advise you.

We aim to ensure consent is current, specific, fully informed and provided voluntarily and by someone with capacity.

We will provide you with the option not to identify yourself or to use a pseudonym, however in some situations this will often compromise or limit the service we can provide.

If we receive unsolicited personal information (e.g. misdirected mail or email) we will act based on method of receipt, reasonable necessity for and sensitive nature of the information, and either destroy or de-identify the information as soon as practicable, if it is lawful and reasonable to do so, or notify you and act in accordance with privacy laws and our policy and procedure.

How we store and manage personal information

Personal information we hold is stored electronically in secure IT systems and some information is stored in paper files.

We take all legally required and commercially reasonable measures, proportional to the associated risk, to protect personal data stored physically and electronically from loss, interference, misuse, unauthorised access, modification or disclosure.

To help protect the security of your personal information we will de-identify your information in certain circumstances.

Our records retention policies and procedures detail how we keep personal data no longer than necessary or permitted by law.

Disclosing your personal information

We take all legally required and commercially reasonable steps to ensure the personal information we collect and disclose is accurate, up to date and the information we disclose has regard for the purpose of use or disclosure.

We take all reasonable steps to disclose personal information:

- only if we have received consent to do so; or
- if required or authorised by any Act, law or legislative and statutory requirement; or
- where there is a public duty to do so; or
- an individual's health or safety is at risk; or
- we are required to exchange information for purposes such as employment; or
- are otherwise required or permitted to disclose the information under the Privacy Act or legislation.

Where we obtain consent to share information with others we will explain with who, why and what those organisations will do with the data. We will give you the choice to do this at the time we collect your information and will record the conditions of the agreement.

We will always advise you of steps we must take to protect your privacy before any of your personal information is disclosed overseas.

Access to and correction of your personal information

- Unless a specific exemption applies, we will give you reasonable access to your personal data and, as appropriate, the ability to correct, delete, or update inaccurate or incomplete information.
- If you wish to gain access to your personal information stored with Community Gateway you must make the request in writing to the CEO. Requests will be acknowledged within 7 days and the information provided within 30 days from original request date.
- If you who wish to correct your personal information stored with the Community Gateway you must make the request in writing to the CEO. Requests will be acknowledged within 7 days, and as relevant the data updated within 14 days from original request date.
- If you wish to raise a privacy concern you should contact the CEO by email ceo@nrcg.org or by writing to PO Box 525 Lismore NSW 2480.

Procedure:

The Community Gateway will collect, hold and use personal data about an individual only as permitted or required by applicable laws and in accordance with the following procedure.

Client information

Record-keeping and sharing practice

1. Information on clients should be as non-obtrusive and objective as possible, yet relevant and up to date.

2. As per the Privacy Principles, consent should be current and specific, and sought for collection, proposed use and disclosure at the time the information is collected.

Client consent

Community Gateway consent – ChilliDB record

1. At point of intake clients are provided with an organisation-wide consent request as part of establishing the client record in ChilliDB. The standardised script should be read or otherwise communicated to all clients. This consent covers Community Gateway obligations to report in the Data Exchange (DEX) and to similarly use de-identified information for organisational research from time to time. Refer *ChilliDB Privacy and Consent Script*.
2. Functionality within ChilliDB enables an historical log of details of consent and if relevant, withdrawal. Staff should refer to the latest ChilliDB manuals for detail.
3. Where no client record has yet been established in ChilliDB during program intake the caseworker may use the *Intake and Assessment Form* to record Community Gateway consent (including presenting the *ChilliDB Privacy and Consent Script)* and record this with other client mandatory information in ChilliDB.

Program specific consent

1. Program specific consent is obtained at point of program intake. For Helping Hands, Connecting Families, ROSAS and Trauma Counselling programs use the *Consent for Casework Services Form*. This form is applicable to adults and young people.
2. To record consent for external parties and referral exchange across all programs practitioners should use the *Consent for Casework Services Form* which provides a listing format for third parties and referral services. Consent is not required for internal referral.
3. To record clients consent to counselling services practitioners should use to the *Consent for Casework Services Form* and scan to ChilliDB. This form caters for both adult and young people.

Capacity

1. When obtaining consent from a client who is a child, it is best practice to seek consent from the child's parent or guardian, except in circumstances where it is considered the child has sufficient understanding and maturity to understand what is being proposed. As a general rule, the Community Gateway may presume that an individual aged 15 or over has capacity to consent, unless there is something to suggest otherwise. An individual aged under 15 is presumed not to have capacity to consent.
2. When obtaining consent from a client whose capacity to consent may be compromised (e.g. a client with a physical or mental disability or limited understanding of English or temporary incapacity), it may be appropriate to consider who can provide consent on the client's behalf. Options include a guardian, someone with an enduring power of attorney, a person recognised by other relevant laws (e.g. a 'person responsible' under the *Guardianship Act 1987* (NSW)) or a person nominated in writing by the client while they were capable of giving consent.
3. If the client can give consent but cannot write, somebody else who can write can sign as a witness to the client's verbal consent.
4. While individuals have the right not to identify themselves when dealing with the organisation, for many programs it may not be reasonably practical to provide service if adequate personal information is not provided.
5. A client has the right to withdraw or restrict their consent to release personal information at any time. This request may be verbal or in writing.

Anonymity

1. There are limited circumstances where it may be possible to deal with the Community Gateway anonymously or using a pseudonym, such as clients seeking general information about services. In most cases it will not be possible to deal in this way due to information and identifiers required by regulators and agencies.

Employee information

1. The Community Gateway collects personal information from prospective employees, contractors, and volunteers. Australian Privacy Principles apply to this information.
2. It collects and holds personal information in relation to its current employees and other workplace participants (including volunteer workers). For example tax file number, information relating to personal background, work and remuneration of workplace participants.

3. While information handling of employee records that directly relate a person's current or former employment relationship are exempt from Australian Privacy Principles, this does not extend to after hour behaviour or social media or other records not related to employment with the organisation.
4. Staff/workplace participant information is to be stored electronically wherever possible or otherwise in a filing cabinet which is kept locked when the office is unattended. The information is only accessible to the Chief Executive Officer (CEO) and other staff members delegated by the CEO.

Reasons why information is held

1. There are a variety of reasons why the Community Gateway is required to hold information on employees and other workplace participants, including:
    - ensuring both the organisation and any workplace participants are meeting their obligations under relevant legislation as well as their contract, if employed
    - ensuring the health, safety and welfare of all workplace participants at times when they are performing work
    - allowing appropriate insurance for these workplace participants.
2. There may be certain circumstances where the Community Gateway is contacted in relation to personal information. For example, when an employee has applied for a loan with a financial institution and that institution contacts the organisation to verify details of income. The employee should contact the Manager – Corporate Services and give verbal or written consent for the release of the requested information.

Permitted situations

1. The *Privacy Act* sets out certain permitted situations that allow for collection, use or disclosure of personal information (including sensitive and health) in special circumstances.
2. For example, the organisation may be compelled to disclose information about a client if:
    - legislation requires information to be released
    - a person or the organisation is subpoenaed to provide information for court proceedings

- if at risk of harm to self or others.

3. For example, the Community Gateway may be compelled to disclose information about a staff member without consent if:
    - legislation requires information to be released
    - there is an overriding public interest (e.g. a duty to warn a third party who is in danger)
    - a person or the organisation is subpoenaed to provide information for court proceedings.
4. An overview of some of the most likely situations to apply to the Community Gateway are detailed in the *Appendix: Permitted Situations Quick Reference* (produced by *Not for Profit Law*).
5. Staff should always consult with their manager regarding any circumstances of information sharing without consent, including in a matter of legal requirement, or in consideration of risk of safety and well-being of client and others who may be affected by their actions.
6. The CEO is the responsible person in these matters and managers and staff must act under the direction of the CEO.

Public communication of policy

1. Community Gateway will make its *Privacy and Confidentiality Policy* statement and guidelines available publicly via its website.
2. In accordance with APP it will use a layered approach to assist understanding. A layered approach means providing a condensed version of the full policy to outline key information, with direct links to the more detailed information.
3. Statement and guidelines will be written in clear language and include contact details for queries, concerns or complaints.

Methods of management

Community Gateway will maintain the following information and data management practices:

1. Periodic review of the adequacy of existing physical and electronic security measures and procedures, including whether any relevant standards are met.
2. Ensure all staff and volunteers who have access to people's information and data understand the organisation's policies and procedures and are trained in privacy, confidentiality and information sharing practices and procedures.
3. Maintain a system of access restrictions (electronic and physical) with individual permission levels approved only by the CEO.
4. Record audit trails to access documents and personal information where possible.
5. Place computer screens out of view of others, particularly visitors to the organisation, and ensure screens are locked when unattended.
6. Ensure adequate IT security, such as firewalls and anti-virus scanners on work IT systems per its information technology and data policy and procedure.
7. Check all personal information has been removed from electronic devices before decommissioning or destroying them.
8. Keep hard copy files in properly secured cabinets and develop practices to limit the need for paper-based collection and storage where possible.
9. Restrict printing of electronically stored personal data.
10. Restrict staff access to personal information on a 'need to know' basis only.
11. Regularly monitoring information handling practices to ensure they are secure.
12. Follow record keeping practices pursuant to legal and statutory retention and destruction requirements. See *Recordkeeping, Archive and Storage Policy.*
13. Shred, pulp or otherwise destroy personal information paper records (e.g. dispose of files in security bins).
14. Delete electronic records or files securely so that they can't be retrieved.

Complaints

1. Any client, employee or workplace participant who feels there has been unwarranted invasion of their privacy should follow the *External Complaints* or *Staff Grievances* policies, as relevant.

Data breach response

See *Data Breach Procedure*.

External providers and contract

1. The Community Gateway will ensure any third parties who manage the organisation's information and data have policies and procedures that meet the legal requirements and expectations of the organisation.
2. Organisations may be required to sign a *Contractor Confidentiality Agreement* or *Non-Disclosure Agreement*.
3. Ensure all contracts with third party providers, including cloud storage, indicates where the data is stored and if this involves overseas storage.
4. Contracts and agreements will be periodically reviewed for privacy law impact and obligations.

Additional resources

Privacy resources for private NSW health providers, NSW Information and Privacy Commission

Privacy guide, Not for Profit Law.

Client point of contact	Process step	Form, mechanism	External communications

New client	Consent for DEX and Community Gateway research and storage in ChilliDB	Read *Privacy and consent script* directly from ChilliDB and check boxes x 2 OR If using *Intake and assessment paper form* and client not already in ChilliDB – caseworker reads printed script and completes consent questions, data later entered in ChilliDB	Website – privacy policy statement and guiding principles + link in footer on each page Privacy policy statement available to print from SharePoint and provide on request Client rights and responsibilities card Phone on hold may mention privacy statement is available on website
New casework client (already in ChilliDB) Trauma counselling, ROSAS, Helping Hands, Connecting Families	Consent for program specific information sharing, client's nominated third parties, consent for counselling services (if relevant)	*Consent for casework form*	
	Information exchange provisions under Chapter 16A of the Children and Young Persons (Care and Protection) Act 1998	*Chapter 16A letter proformas* and factsheets on SharePoint	RRK Family Handbook
Rainbow Region Kids	Consent for Xplor and Community Gateway research and storage in ChilliDB	*Rainbow Region Kids enrolment form*	
	Third party consent	*NSW Inclusion Agency form* *DESE Permission to Share form*	

NILS	Client consent	Procedure and guides as dictated by Centrelink and Good Shephard Microfinance	
Trauma counselling online referral	Website surveys feed into ChillDB		
Internal referral	Record in ChilliDB, no further consent required		