Policies and Procedures
Organisation

Privacy and Confidentiality Policy

NCNS
NEPEAN COMMUNITY & NEIGHBOURHOOD SERVICES

Contents

Policies and Procedures
Organisation

Privacy and Confidentiality Policy

Policy Statement

Nepean Community & Neighbourhood Services (NCNS) 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 NCNS 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.

This policy applies to the internal records, Client records and unpublished materials of NCNS.

Scope

This policy applies to all Board members, staff, volunteers and students of NCNS.

Policy context

This policy relates to:

Legislation	Privacy Act (1988) (Cth) Privacy Amendment (Notifiable Data Breaches) Act 2017 Australian Privacy Principles Children Legislation Amendment (Wood Inquiry Recommendations) Act 2009 Children and Young Persons (Care and Protection) Act 1998
Organisation policies	See under 'Related documents'

Policy principles

NCNS is committed to transparency in its operations and to ensuring it is open to public scrutiny. It must also balance this with upholding the rights of individuals to privacy and of the organisation to confidentiality on sensitive corporate matters.

The principles supporting high-quality confidentiality practices at NCNS are:

- Confidentiality – confidentiality practices are applied consistently across the organisation and are accessible for clients
- Privacy - only information necessary for the delivery of high-quality services is collected and stored by NCNS
- Dignity - NCNS respects and protects clients' dignity and right to privacy
- Consent - information is only shared externally with consent or where required by law
- Experienced – the team is appropriately skilled and qualified to oversee and manage our organisation's Privacy and Confidentiality Policy.

Definitions

Confidentiality	The protection of personal information. This means keeping someone's personal information between you and them, and not telling anyone else unless they have given you informed consent to do so, unless authorised by legislation. It also means that client information is kept securely by NCNS.
Privacy	Respecting a client's personal and physical privacy, dignity and uniqueness, such as having a private space in which to speak about their needs or issues.
Personal Information	Personal information can include – • name, date and place of birth • race or ethnicity • financial/banking details • health/diagnostic information • employment details • organisational information, such as business conducted in Board meetings, competitive tenders or expressions of interest, and client information • photograph (including CCTV footage) • signature • uniquely identifying number – e.g. driver license number, tax file number, employee number • details of services requested or obtained • unique physical characteristics – e.g. tattoo, birthmark. Personal information can also include information provided through workplace processes, such as in the course of performance reviews, leave applications, supervision sessions or similar discussions, and Information about any internal dispute or grievance. Personal information may reveal a person's identity even if their name is not mentioned. Other information may enable their identity to be deduced.

Data breach	When personal information is disclosed accidentally, lost, or accessed without permission. This may happen due to human error, or by malicious action.

Procedures

1. Commitment to privacy legislation

NCNS processes for the collection, storage, use and disclosure of personal information comply with the obligations of the *Privacy Act 1988*, and in accordance with the Australian Privacy Principles. These obligations are:

- telling individuals of their right to know why information is collected, how it is protected, how it is stored, how long it is kept, how it is disposed of, how they can access their personal information
- seeking consent from individuals for the collection, storage, use and disclosure of personal data
- only collecting information that is appropriate and relevant to the provision of services or for its primary function
- ensuring individuals can make corrections to their personal information, where necessary unless access is refused by law
- taking all reasonable steps to store personal information securely and protect it from misuse, loss, unauthorised access, modification, or disclosure.

2. Privacy protection

- NCNS has controls in place to protect the security and privacy of the information we hold for clients, Board members, management, staff and volunteers.
- All Board members, management, staff and volunteers sign a Confidentiality Agreement, the Code of Conduct and the Code of Ethics when they commence at our organisation.
- All Board members, management, staff and volunteers are trained on our legal obligations for privacy and confidentiality.

- NCNS seeks consent from individuals for the collection, storage, use and disclosure of personal data (refer to the *'Client Information and Consent Form: Collecting and Releasing Personal Information'*).
- When meeting with clients we arrange for a private meeting space for interviews and when talking about matters of a sensitive or personal nature.
- The *'Client Information and Consent Form: Collecting and Releasing Personal Information'* explains the client's right to withdraw their consent at any time.

3. Client personal information

3.1 Collection of client personal information

3.1.1 We only collect information that is necessary for effective service provision, including assessments.

All personal information will be stored securely – paper files in a locked filing cabinet, and electronic files digitally, accessible only to those who need it.

3.1.2 Client information will only be discussed between staff in order to perform their role effectively.

3.1.3 All clients will be informed how and why their information is used and stored, and how they can access their personal information and correct it.

3.1.4 Only factual and relevant information required to provide effective service, and to meet funding body requirements, will be collected and stored.

3.1.5 It is the responsibility of staff to take into consideration the client's cultural and linguistic needs, and any disabilities that may impact understanding, and deal with these appropriately.

3.1.6 Where a client is being referred to other services, a '*Client Information and Consent Form: Collecting and releasing Personal Information'* must be completed by the client, or a verbal approval may be requested from the client and documented.

3.1.7 A client has the right to withdraw consent to the release of personal information at any time.

3.2 Sharing of personal information

Personal information is only shared verbally or in writing with the client's written consent unless the circumstances are such that limits to confidentiality apply.

3.3 When we can release your information without your consent

There are circumstances in which client information may be shared without the consent of the client:

- Upon subpoena to produce documents or give evidence in court
- Under Section 248 of the *Children and Young Persons (Care and Protection) Act 1998*, where the NSW Department of Communities and Justice can prescribe agencies to provide information about the safety and well-being of children
- Under Chapter 16A of the *Children Legislation Amendment (Wood Inquiry Recommendations) Act 2009*, which allows for information to be shared between prescribed bodies to assist with responding to the safety, well-being and welfare of a child or young person.
- Where there are reasonable grounds to believe a person is at risk of harming themselves or other, or that a serious criminal offence has or will be committed

Any information requests should be in writing.

In any of these circumstances, NCNS will endeavour to advise clients of our action, unless this would pose a risk to staff.

3.4 Accessing client records

All clients have the right to access their records and advise the organisation about inaccuracies. NCNS undertakes to ensure access is:

- convenient
- without reasonable delay
- without cost.

Requests for information about clients from outside agencies or individuals will be referred to the Managing Director. Before any information is released, the Managing Director or delegate will contact the client concerned to obtain consent.

3.5 Moving physical client records

Physical client records can only be removed from work premises in a secure manner:

- in line with archiving procedures
- as a result of a court order
- for transfer to another project
- to be returned to the client
- when moving premises

4. Child safety and protection

Relevant entities in NSW must report allegations and findings of sexual offences, sexual misconduct, ill-treatment of a child, neglect of a child, an assault against a child, failure to protect a child or failure to report if a child has been harmed, as well as any behaviour that causes significant emotional or psychological harm to a child.

NCNS is committed to the early detection and taking action on children and young people suspected to be at risk of harm and the prompt reporting of children at risk of **significant** harm (ROSH).

In terms of child safety, there are circumstances in which client information may be shared without the consent of the client:

- under Section 248 of the *Children and Young Persons (Care and Protection) Act 1998*, where the Department of Justice and Communities can prescribe agencies to provide information about the safety and well-being of children
- under Chapter 16A of the *Children Legislation Amendment (Wood Inquiry Recommendations) Act 2009*, which allows for information to be shared between prescribed bodies to assist with responding to the safety, well-being and welfare of a child or young person.

For more information, please see the NCNS Child Safe (Safety and Protection) Policy.

5. Request for access – general records

Any request for access to information should be referred to the Managing Director who will:

- make available to staff or Board members information that they are entitled to access

- refer any request from the public for access to NCNS records or materials to the Managing Director

In considering a request, the Managing Director will take into consideration:

- the business, legal and administrative interests of NCNS, including commercial confidentiality and privacy obligations.

6. Staff Information

- All personal information of staff will be stored in their staff file in a securely locked filing cabinet at NCNS central office.
- Staff information will only be discussed with other staff in order to perform their roles effectively.
- Staff may request their information be disclosed to other staff.
- Electronic staff information may be stored securely, accessible only to those who require it to perform their role effectively.
- If a staff member, volunteer or student becomes aware of an issue concerning someone they are working with, this information may only be shared with their supervisor, and must not be shared outside the organisation.

7. Staff responsibilities and commitment

Confidential information and NCNS

During the course of your employment or engagement with NCNS, you may become aware of information and material relating to the affairs and operations of NCNS, its staff, clients, program participants, service partners, consumers of our services and community members. This information is confidential; during and after your employment, you must therefore:

- keep all Confidential Information secret and confidential
- take all reasonable and necessary precautions to maintain the secrecy and prevent the disclosure of any Confidential Information
- not disclose any Confidential Information to any third party
- not use any part of or make copies of any Confidential Information, except:
    - as reasonably required in the ordinary and proper course of your employment;

- to the extent required by law; or
- if written consent from NCNS is first obtained

- ensure that client files and data are kept locked and not accessible when not in use

Confidential information means any information relating to the business or affairs of NCNS, its clients, stakeholders, contractors, staff paid and unpaid, that is not in the public domain including, but not limited to, any document, record, computer file, lists of current or former clients, trade secrets, customer or client details and information, product or service information, teaching methods, sales and marketing information, lists of prospective clients or customers, information relating to any computer systems or software, financial information, discovery, invention, drawing, design, strategy, plan, data, report, process, proposal, budget, idea, concept or know how.

The requirement to maintain confidential information will survive the termination of your employment, irrespective of the basis of the termination, and shall remain in full force and effect indefinitely.

What staff need to do

All staff will:

- retain all confidential information in the strictest confidence and not disclose any confidential information to any person other than for purposes directly related to their position at NCNS
- not use any confidential information which they have acquired in relation to the activities of NCNS for their own interests or the interests or purposes of others not associated with NCNS
- not make copies of any confidential information for any other reason other than those essential to and directly related to their position and responsibilities with NCNS
- upon the request, and in any event upon the cessation of their engagement or employment with NCNS, return or destroy materials containing confidential information which are in their possession

This will not prevent an individual from:

- disclosing information to proper authorities in relation to concerns about improper conduct, breaches of laws or breaches of duty of care
- providing access for external reviewers to de-identified information for the purposes of formal audit processes
- making a formal complaint to appropriate authorities about an aspect of

the organisation's operation

- disclosing any information that they may be required to disclose by any court or regulatory body or under applicable law

8. Managing Privacy Breaches

- Legislation requires NCNS to report any data breach that is likely to result in serious harm to the people whose information is involved.
- If a breach occurs, the Managing Director and/or Operations Manager will take steps to:
  - identify the breach
  - limit the potential harm (such as by shutting down the system)
  - notify clients whose personal information is involved
  - assess whether further investigation is necessary, and if so, notify the Office of the Australian Information Commissioner, as per their guidelines
  - take remedial action, and implement measures to ensure it doesn't reoccur
  - record all details in a Data Breach Log and review.

9. Privacy and Confidentiality complaints

To make a complaint or raise a concern about NCNS's privacy and confidentiality practices and processes:

- Call 02 4721 8520 and ask to speak to the Managing Director or the Operations Manager
- Email info@nepeancommunity.org.au
- Refer to the Complaints Resolution & Feedback Policy and complete a 'Complaints Feedback Form', or write to us at Nepean Community & Neighbourhood Services, PO Box 7599, South Penrith 2750, or by email to: manager@nepeancommunity.org.au
- If you don't feel comfortable speaking with us or writing to us with your complaint, you, a friend or support person can contact the NSW Ombudsman. The Ombudsman is an independent watchdog whose job is to protect the rights of people using or accessing community service providers. You can discuss your complaint with them:
  - NSW Ombudsman: 1800 451 524 or (02) 9286 1000 or nswombo@ombo.nsw.gov.au or www.ombo.nsw.gov.au

Related Documents

NCNS Policies:

- Child Safe (Safety and Protection) Policy
- Client Services Policy
- Code of Conduct
- Code of Ethics
- Complaints Resolution & Feedback Policy
- Records Management Policy

NCNS Forms, record keeping, other documents:

- Client Information and Consent Form: Collecting and Releasing Personal Information
- Client Registration Form
- Data Breach Log

Policy Review

Version	Date reviewed	Amendment notes	Next Review Date
V.1	February 2007		February 2009
Review	October 2009		October 2011
Review	November 2013		November 2015
Review	June 2016		January 2020
V.2 Review	November / December 2022	Formatting and text review.	
V.2 Recommended	December 2022	Reviewed, amended and recommended by Policy Subcommittee 7 December 2022.	
V.2 Ratified	April 2023	Ratified by the Board 19 April 2023.	April 2025

Date

19 April 2023