# PRIVACY & CONFIDENTIALITY POLICY

| | |
|---|---|
| Section 1: Service Management and Governance | |
| Policy number: 1.7 Authorised by: Management Committee | |
| Date adopted: 29th July 2013 | Date last reviewed: January 2026<br>Next review Due: April 2028 |
| **Related Standards** | |
| Human Services Quality Standards<br>Standard 1: Governance and Management<br>Standard 2: Service Access<br>Standard 4: Safety, Wellbeing and Rights<br>Standard 5: Feedback, Complaints and Appeals | National Accreditation Scheme Standards<br>Standard 3 – Staffing, including Volunteers<br>Standard 5 – Organisational Risk Management and Compliance<br>Standard 6 – Management of Information and Data |

***Purpose***

Northside Connect Inc (NCI) respects the privacy and confidentiality of all stakeholders, including clients, staff, volunteers, students, members, customers, the organisation and is committed to safeguarding personal, sensitive and health information provided to us. This policy outlines how NCI handles confidentiality and information, what information is collected and why, how an individual can access and correct their information, how NCI adheres to the notifiable data breaches scheme and our complaints process.

The Privacy & Confidentiality Policy is to be placed on NCI's website, to be available at NCI's premises and included in induction materials provided to volunteers, staff and other appropriate recipients. In addition, the Privacy Collection Notice is also to be affixed in the public area of NCI's premises, if appropriate, individual offices and available to the public when making enquires via NCI's website.

***Policy statement***

NCI aims to uphold, to the highest standard, the rights of all stakeholders to confidentiality and privacy in accordance the principles embodied in the Privacy Act 1988 [Cth], the Australian Privacy Principles, the Information Privacy Act 2009 (Qld) and the Qld Privacy Principles (QPPs). This policy will apply to all records, whether hard copy or electronic, containing personal and sensitive information (and if applicable, health information) about individuals and other stakeholders (but does not apply to acts and practices of current or former employees' records). Training will be provided to appropriate staff, students and volunteers during induction.

***Definitions***

**Personal Information**: 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.

Personal information may include:

- Names and significant dates including dates of birth, death, marriage/ cohabitation or separation
- Contact details including postal, street, phone and email
- Demographic information such as age, gender, relationship status and finances
- Information relating to referrals made to and from the NCI

- Information collected from you or other as a result of your access to our services
- Other information that we are required to collect by our funders or others (e.g. statutory bodies) or to provide services
- English proficiency, need for an interpreter or disability
- Feedback from you on services provided

**Sensitive Information**: 'Sensitive information' is defined in the Privacy Act to mean information or an opinion about an individual's, racial or ethic original, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual preferences or practices or criminal record.

**Health information** is a part of an individual's personal and sensitive information and includes information or an opinion about a person's health or disability. Health information is only collected if directly related to, the activities and functions provided by NCI.

**Data breach** is when personal information held by an entity is lost or subjected to unauthorised access, modification, disclosure, or other misuse or interference. Examples of a data breach are when a device containing personal information of clients is lost or stolen, an entity's database containing personal information is hacked or an entity mistakenly provides personal information to the wrong person

***Collection of your information***

**Information -** NCI will only collect your information for the purpose of providing services. The main way we collect information about you is when you give it to us. On occasion NCI may obtain information from a third party source (e.g. from a referral). In such instances, NCI will take reasonable steps to contact the individual to ensure they are aware of the purpose for which we are collecting information. NCI will:

- Only collect information that is relevant to the NCI'S primary functions.
- Inform the individual why information is being collected, for what purpose it will be used and who will be able to access that information.
- Inform the individual that their information will only be shared with others with their consent, in the circumstance hereunder or otherwise as provided by law.
- Ensure that information is only collected by fair and lawful means.
- Ensure that the collection of information does not intrude to an unreasonable extent upon the personal affairs of the individual involved.
- Take reasonable steps to protect all staff, volunteer and client records from misuse, interference and loss, and from unauthorised access, modification or disclosure.
- Provide individuals with access to their own records.
- Ensure that personal information collected or disclosed is accurate, complete and up-to-date, and provide access to any individual to review information or correct wrong information about themselves.
- Advise that if they are unhappy with how NCI has managed their privacy, they have the right to pursue these concerns via the complaints policy.

Other than the primary purpose for which information is being collected, we may also disclose your information to other external organisations including:

- to government departments/agencies who provide funding for NCI services
- if you are a legal client, your deidentified information with Community Legal Centres Australia through their community legal services system for reporting, funding and law reform purposes
- contractors who manage or maintain some of the services we offer
- IT services (e.g. our IT support provider, web host etc.)
- translator services

- other regulatory bodies, such as WorkSafe
- referees and former employers of NCI employees and volunteers, and candidates for NCI employee and volunteer positions
- our insurers
- our professional advisors, including our accountants, auditors and lawyers.
- NCI does not use or disclose personal information for direct marketing purposes. However, on occasion NCI will take photographs and videos at events for use on the NCI website, social media, media and other publications. If you do not wish your photograph taken, please advise a staff member.

***Anonymity***

We generally require your details to provide legal advice at BNCLS to ensure we meet our ethical obligations as solicitors and comply with practice guidelines. We also generally require your details for our counselling or DFV programs to ensure we meet our ethical requirements. Only in very limited circumstances are we able to provide legal advice or counselling anonymously or without full client details.

However, we will allow you to interact with us anonymously or using a pseudonym where possible. For example, if you contact our general office number with a general question, or for safety reasons do not wish to be identified, we will not request your name or other personal information unless we need it to adequately assist you.

***Indirect collection***

While assisting you, we may collect information about you indirectly from publicly available sources or from third parties (such as experts or witnesses). We will only collect information about you from publicly available sources and/or third parties in legal matters where you would reasonably expect us to do so or with your consent.

***Storage & Security of information***

All Management Committee members, staff, volunteers and students will read and sign a Code of Conduct on commencement with NCI. All newcomers to NCI are to be trained in the induction process on the necessity of confidentiality and privacy.

Subject to the Coordinator's overall responsibility and that of the Principal Solicitor under professional obligations, all staff and volunteers are responsible for the management of information to which they have access and used in the conduct of their work.

All information will be securely stored in locked cabinets and/or password protected databases with access restricted to those who require it to work with clients and to carry out the services of NCI i.e. on a "need to know" basis.

The Coordinator is responsible for safeguarding personal information relating to NCI staff, Management Committee members, volunteers and members and will handle client complaints about privacy.

Information recorded on the Legal Service Customer Management System for the purposes of conflict checking will be password secure and only approved staff who have undergone Legal Service induction training will be allowed access.

All personal and sensitive information will be destroyed after minimum legal requirements for retaining documents have expired.

Whenever NCI receives unsolicited personal information, it will determine whether it would have been permitted to collect the information under Australian Privacy Principle 3. If so, then the provisions of APP 5 and APP 13 will apply to that information. If the information could not have been collected under APP 3,

and the information is not contained in a Commonwealth record, NCI will destroy or de-identify that information as soon as practicable, if it is lawful and reasonable to do so.

It is the responsibility of staff to ensure privacy protocols are maintained and a confidential environment is maintained by:

- ensuring contacts with clients and formal staff supervision sessions are conducted in spaces that provide for privacy and confidentiality
- all conversations regarding confidential personal or sensitive information should be conducted in private and only with appropriate persons.
- ensuring that staff do not discuss clients in public, during breaks and outside work time and communal areas (e.g. hallways, reception, cafes, restaurants, etc.)
- adhering to the clear desk policy: client, HR and supervision files are kept in locked filing cabinets, and returned to the cabinet immediately after use. No files/paperwork is to be left unattended on desks, nor stored in staff member's diaries or in-trays.
- computer screens are turned away from the public etc and electronic calendar appointments shall refer only to the client's "LAST NAME", with their details in the body of the item
- keys to cabinets holding information should not be kept in an obvious place such as a top drawer.

***Staff, student and volunteer records***

In protecting the privacy of the information of staff, students and volunteers [including Management Committee members], NCI will ensure the following:

- All individuals will be allocated their own personnel file which will contain all personal information and be held in a secure location on site.
- No personal information will be released to a third party including other volunteers or staff without the permission of the individual.

Release of work-related information such as work email address, current whereabouts etc must be authorised by an appropriate staff member prior to releasing this information. This information will only be released under exceptional circumstances.

From time to time the Organisation may send information to volunteers, students and staff on events and activities being held at the Centre. Individuals will always be given the option of opting out of this.

***Use of Information/Limits to Privacy***

All personal and/or sensitive information gathered during the provision of services will remain confidential and secure as per the Client Record Keeping Policy, except when:

- the individual and/or client expressly provides consent
- you would reasonably expect us to use or give that information for another purpose related to the purpose for which it was collected (or in the case of sensitive information – directly related to the purpose for which it was collected)
- required or authorised by law for example subpoenaed by a court of law or necessary to assist in law enforcement
- where there is a duty of care to lessen or prevent a serious and imminent threat to the life, health or safety of the client or any individual or to public health or safety and failure to disclose information would place that person at further harm. Such cases should be immediately discussed with the Coordinator and/or Principal Solicitor as to whether disclosure is necessary
- it is reasonably necessary for us to take appropriate action in relation to suspected unlawful activity, or misconduct of a serious nature that relates to our functions or activities
- to assist in locating a person who has been reported as missing other than where the client is seeking advice from the BNCLS on such issue not involving the NCI
- it is reasonably necessary to establish, exercise or defend a claim at law
- it is reasonably necessary for a confidential dispute resolution process

- where unlawful activity or fraud is suspected other than where the client is seeking advice from the BNCLS on such issue not involving the NCI
- approval of the client has been obtained to release information to another party
- the case is being reviewed for the purpose of professional supervision, in which case all identifying information will be removed prior to review
- when required by relevant authorities under the Legal Profession Act 2007 (Qld)
- it is necessary for the management, funding or monitoring of a health service relevant to public health or public safety
- it is necessary for research or the compilation or analysis of statistics relevant to public health or public safety
- it is reasonably necessary for the enforcement of a law conducted by an enforcement body

In sharing information regarding clients, NCI will ensure that the following steps are taken:

- Providing clients with information on our Privacy and Confidentiality Policy and Procedures on commencement of services. For those clients seeking individual assistance through BNCLS or the Domestic Violence Program they will be required to acknowledge they have been provided with this information, including the right to access the full privacy policy.
- Having a "Consent for Information Sharing" form which clients can sign on an as needed basis. Permission may also be given verbally in cases where the client is unable to sign a Consent for Information Sharing form. Staff must explain this form to clients and how it will be used. Staff must not enter any new information on this form after the client has signed, unless permission is sought from the client.

***Disclosure of personal information to overseas recipients***

We do not usually send personal information out of Australia. If we are otherwise required to send information overseas, we will take measures to protect your personal information.

***NCI Website and Social Media***

Our website may use cookies or similar tracking technologies to understand how the site is used and to help improve user experience. You can disable cookies through your browser settings; however, doing so may affect how the website functions. We do not attempt to identify individuals who visit our website. Where our website or social media platforms contain links to external government or non-government sites, NCI is not responsible for the privacy practices, security, or content of those third-party sites. Your activity on those sites is governed by their own privacy policies.

We will only collect your name, phone number, email address, or contact details if you choose to send us a message. This information will be used solely for the purpose for which you provided it. We will not use your email or contact details for any other purpose, nor will we share this information with a third party without your consent.

***Donors and Supporters***

NCI collects only the information about donors and supporters that is necessary for us to effectively deliver our services. We record only the information that individuals choose to provide. This information is used to:

- process donations
- send acknowledgements and issue receipts
- respond to enquiries or comments
- provide information requested about NCI
- seek support to continue our work
- obtain feedback to help improve our services

Donors and supporters may opt out of communications from NCI at any time, or choose to change the frequency or type of communications they receive. Please contact us if you wish to make any such changes or require further information.

NCI will never sell, rent, or disclose personal information about donors or supporters to third parties for their use. Personal information will only be shared with third parties where we have the individual's consent or where required by law. We will only publish personal information in our communications or promotional materials with the express permission of the individual.

***Data Breach***

A data breach occurs when personal or sensitive information is lost or accessed, used, modified, or disclosed without authorisation. NCI has established a data breach reporting and response plan to reduce the risk of harm to anyone whose information may be affected.

In summary, our data breach reporting and response plan:

- outlines the responsibilities of staff when a data breach or suspected breach occurs, including the steps they must follow
- appoints a dedicated data breach response team
- sets out strategies for containing, assessing, and managing data breaches
- specifies the process for notifying affected individuals and relevant authorities in the case of an eligible data breach
- details the review procedures that help prevent future breaches

If we determine that your personal or sensitive information has been involved in an eligible data breach, we will notify you in accordance with the Notifiable Data Breach Scheme under the Privacy Act.

***Right To Access/Correct information***

Individuals have a general right of access to their own personal information after their identity is confirmed and have the right to have that information corrected if it is inaccurate, incomplete or out of date.

If you ask, we must give you access to your personal information and take reasonable steps to correct it if we consider it is incorrect, unless there is a law that allows or requires us not to/exceptions as noted below. If we make a correction and we have previously disclosed the incorrect information to others, you can ask us to tell them about the correction. We must do so unless there is a valid reason not to.

The request to access personal information is to be made in writing using the Client Request to Access Information Form. The request may also be given verbally in cases where the client is unable to sign the form. In this circumstance a senior staff member must be present when the verbal request is made.

The request will be considered by the Coordinator and, if there are no legitimate barriers to accessing the information, the information will be made available. If the request is denied, NCI will provide a written reason for the refusal and advise of available complaint mechanisms. Should people remain dissatisfied they may exercise their rights under the organisation's Complaints Policy.

Access may be denied or limited for the following reasons:

- access would pose a threat to the life or health of any individual
- privacy of others may be affected
- the request is frivolous or vexatious
- information relates to existing or anticipated legal proceedings
- access would prejudice negotiations with the individual
- access would be unlawful
- denying access is required or authorised by or under a law
- commercially sensitive information
- access would prejudice law enforcement activities

- access would prejudice an action in relation to suspected unlawful activity, or misconduct of a serious nature relating to the functions or activities of NCI
- any other reason that is provided for in the APP's or in the Privacy Act.

If we deny access to information, we will set our reasons for denying access. Where there is a dispute about your right of access to information or forms of access, this will be dealt with in accordance with the NCI complaints policy.

***BNCLS - Legal Professional Privilege (LPP)***

It is important to distinguish between confidentiality and legal professional privilege. Both concepts aim to protect information shared between lawyers/clients, but they are distinct in their application. Confidentiality is a broader ethical duty that applies to all information concerning the client's affairs and LPP is a narrower legal doctrine that protects confidential communications between lawyers/clients.

The rationale behind LPP is to promote full and frank disclosure between lawyers/clients. In practice, legal professionals must ensure caution to ensure LPP is not unintentionally waived or breached. Clients of BNCLS often request third parties/support persons to be present in legal meetings. On occasion, BNCLS may also have students, secondees or legal support workers sit in on appointments. Accordingly, BCNLS best practice is to -

1. Ensure no third parties are present unless necessary.
2. If a third party is present, BNCLS may advise the client they may inadvertently waive LPP (i.e. the confidentiality of the advice may be compromised and privileged information may not be protected) and seek client's consent and note consent in the advice.
3. If applicable, note to the third party that the advice is confidential and they should not disclose the information to anyone and note same in the advice.
4. Where appropriate and if sending clients advice mark the advice as "privileged and confidential".
5. Adding information on LPP to induction processes/training as necessary.

***Changes to this Policy***

This policy will be reviewed from time to time or updated prior in accord with further privacy legislation changes.

***Feedback and Complaints***

Please contact the NCI's Coordinator if you wish to make a complaint about NCI's handling of your private information. We will deal with your complaint as outlined in our Complaints Policy, which along with your Privacy Policy is available sending an email to: admin@northsideconnect.org.au. If you are not satisfied with NCI's response a complaint can be made to the office of the Australian Information Commissioner or the Office of Information Commissioner Queensland.