HNS Privacy, Confidentiality and Information Management Statement

Applies to: All staff, volunteers, suppliers and service users	Specific responsibility: Manager and Coordinators responsible for implementation and monitoring.
Date Approved: 01-03-2025	Review Date: 01-03-2027

1. Purpose

Hastings Neighbourhood Services and its related bodies corporate (we, our, us), recognise the importance of protecting the privacy and the rights of individuals in relation to their personal information.

This policy provides guidance on Hastings Neighbourhood Services legal obligations and ethical expectations in relation to privacy and confidentiality.

2. Policy statement

This document is our privacy policy, and it tells you how we collect and manage your personal information.

Hastings Neighbourhood Services is committed to ensuring that information is used in an ethical and responsible manner. Hastings Neighbourhood Services will use its best endeavours to ensure that it meets its legal and ethical obligations as an employer and service provider in relation to protecting the privacy of clients and service personnel.

We respect your rights to privacy under the *Privacy Act 1988 (Cth)* (**Act**) and we comply with all the Act's requirements in respect of the collection, management and disclosure of your personal information. For the remainder of this document the term "your personal information" is pertaining to all information that identifies clients, volunteers, staff, and committee of management members.

3. References

- Health Records and Information Privacy Act 2002 (NSW)
- Chapter 16 A of the Children and Young Persons (Care and Protection) Act 1998 (NSW)
- Part 13 A of the Crimes (Domestic and Family Violence) Act 2007 (NSW)
- Privacy Act 1988 (Cth)
- Privacy Regulation 2013 (Cth)

4. Definitions

What is your personal information?

When used in this privacy policy, the term "personal information" has the meaning given to it in the Act. In general terms, it is any information that can be used to personally identify you. This may include your name, address, telephone number, email address and profession or occupation. If the information we collect personally identifies you, or you are reasonably identifiable from it, the information will be considered personal information.

What personal information do we collect and hold?

We may collect the following types of personal information:-

- Name
- Mailing or street address
- Email address
- Telephone number
- Age or birth date
- Profession, occupation, or job title
- Details of the products and services you have acquired from us or which you have enquired about, together with any additional information necessary to deliver those products and services to respond to your enquiries
- Any addition information relating to you that you provide to us directly through our websites or indirectly through use of our websites or online presence, through our representatives or otherwise, and
- Information you provide to us through our service centre, customer surveys or
- Visits by our representatives from time to time.

We may also collect some information that is not personal information because it does not identify you or anyone else. For example, we may collect anonymous answers to surveys or aggregated information about how users use our website. We may also collect demographic data to provide to our funding bodies such as cultural background, ability needs, languages spoken etc.

How do we collect your personal information?

We collect your personal information directly from you unless it is unreasonable or impracticable to do so. When collecting personal information from you, we may collect in ways including:-

- Through your access and use of our website
- During conversations between you and our representatives
- When you enrol yourself or a child in one of our programs
- When you provide bank details and or complete online links to our data management system
- When you complete an application or purchase order.

We may also collect personal information from third parties including:-

- From third party companies such as credit reporting agencies,
- Law enforcement agencies and other government entities i.e. Working With children Checks or Criminal History Checks for employees and volunteers.

What happens if we cannot collect your personal information?

If you chose not to provide us with the personal information described above, some or all of the following may happen:-

- We may not be able to provide the requested products or services to you either to the same standard or at all

- We may not be able to provide our funding bodies with the required information to acquit our grants and this may impact future services that you may want
- We may be unable to return your enquiry or follow through on a requested referral tailored to your preferences and your experience of our service may not be as enjoyable or useful.

For what purposes do we collect, hold, use and disclose your personal information?

We collect personal information about you so that we can perform our business activities and functions and to provide best possible quality of customer service. We collect, hold, use and disclose your personal information for the following purposes:-

- To provide services to you and to send communications requested by you
- To answer enquiries and provide information or advice about existing and new services
- To provide you with access to protected areas of our website
- To access the performance of the website and to improve the operation of the website
- For the administrative, marketing (including direct marketing), planning, service development, quality control and research purposes of Hastings Neighbourhood Services and all its auspiced bodies.
- To update our records and keep your contact details up to date
- To process and respond to any complaint made by you, and
- To comply with any law, rule, regulation, lawful and binding determination, decision or direction of a regulator, or in co-operation with any governmental authority of Australia.

Who will have access to your information?

Hastings Neighbourhood Services is responsible for the safety and confidentiality of all client files. Client in this case referring to all service users, volunteers and network members. As a condition of employment, all persons entering the employ of Hastings Neighbourhood Services or any of its auspiced services, including all persons engaged in a voluntary capacity, must abide by this policy and its identified procedures. At all times client confidentiality will be adhered to as per the Privacy Act.

No personal information will be shared, sold, rented, or disclosed external to our organisation without signed consent from the individual, other than as described in this Privacy Policy as “de-identified demographic data”.

- Our employees, volunteers or auspiced service providers will have monitored access to your information for the purposes of providing person centred, one door policy service experiences to ensure you are not required to repeat your information every time you access a different program within our service system.
- All staff and volunteers are required to sign a confidentiality agreement on commencement of employment. Any breach of confidentiality may result in dismissal.
- All staff and volunteers are provided with orientation which includes the importance of confidentiality.
- Staff/Volunteers must not directly or indirectly discuss any client, or divulge information concerning any client, to any person except as necessary during the course of their work.
- Copies of, or information contained in, client files requested by other services may only be produced if a letter of authorisation is provided by the client.

- **In matters of child protection concern**, client file information can be shared provided it complies with the child Protection Act where concern for a child's safety warrants a child Protection report. Where information is sort from our agency by and external agency, a letter from the enquiring agency quoting Section 16a of the child protection legislation is provided to the manager. The manager may only share information in response to a specific child protection related enquiry and this must be provided in writing.

How can you access and correct your personal information?

You may request access to any personal information we hold about you at any time by contacting us. Where we hold information that you are entitled to access, we will try to provide you with suitable means of accessing it (for example, by mailing or emailing it to you). We may charge you a fee to cover our administrative and other reasonable costs in providing the information to you.

There may be instances where we cannot grant you access to the personal information we hold. For example, we may need to refuse access if granting access would interfere with the privacy of others of if it would result in a breach of confidentiality. If that happens, we will give you written reasons for any refusal.

If you believe that personal information, we hold about you is incorrect, incomplete or inaccurate, then you may request us to amend it.

Safe storage of information

We take reasonable steps to ensure your personal information is protected from misuse and loss and from unauthorised access, modification, or disclosure. We may hold your information in either electronic or hard copy form. Personal information is destroyed or de-identified when no longer needed.

- Personal details pertaining to clients are kept in locked filing cabinets and/or electronic files with access limited to relevant staff members with password clearance, i.e. those dealing directly with the client, and their supervisors.
- Personal details pertaining to staff and volunteers are kept in locked filing cabinets and/or electronic files with access limited to the HNS Manager and Management Committee.
- All electronic information storage is managed in accordance with our Internet Security, computer and email use policy.

As our website is linked to the internet, and the internet is inherently insecure, we cannot provide any assurance regarding the security of transmission of information you communicate to us online. We also cannot guarantee that the information you supply will not be intercepted while being transmitted over the internet. Accordingly, any personal information or other information which you transmit to us online is transmitted at your own risk.

Our website may contain links to other websites operated by third parties. We make no representations or warranties in relation to the privacy practices of any third party website and we are not responsible for the privacy policies or the content of any third party website. Third party websites are responsible for information you about their own privacy practices.

What is the process for identify or notifying about a breach of privacy?

If you believe that your privacy or the privacy of any service users has been breached, please contact the Manager immediately providing details of the incident so that we can investigate it.

Hastings Neighbourhood Services is responsible for maintaining and monitoring information management systems to ensure early detection of suspected data breaches. Part of this system is for clients, staff and volunteers to be mindful of the policy and report any suspected breaches to the Manager for assessment. Breaches in information security can include an internet "hack", gossip, paperwork being left in unsecure locations and unauthorised sharing of information of any kind.

The assessment of the suspected data breach must be prompt but occur no later than 30 calendar days from the date of suspicion.

The assessment must be incompliance with the Notifiable Data Breaches (NDB) scheme. The NDB schedule in Part111C of the Privacy Act and requires entities to notify affected individuals and the Commissioner of certain data breaches known as 'eligible data breaches'.

An eligible data breach occurs when the following criteria are met:-

- There is unauthorised access to, or disclosure of personal information held by an entity (or information is lost in circumstances where unauthorised access or disclosure is likely to occur).
- This is likely to result in serious harm to any of the individuals to whom the information relates.
- The entity has been unable to prevent the likely risk of serious harm with remedial action.

Entities must also conduct an assessment if it is not clear if a suspected data breach meets these criteria. The assessment will determine whether the breach is an 'eligible data breach' that triggers notification obligations.

5. Procedure

Our procedure for investigating and dealing with privacy breaches is:-

1. To follow the NDBS Data breach preparation and response – A guide to managing data breaches in accordance with the Privacy Act 1988(Cth). The guide includes information about preparing a data breach response plan, assessing a suspected notifiable data breach and responding to a data breach.
2. Initiate: identify the person or group responsible for completing the assessment.
3. Investigate: gather all the relevant information about the data breach, for example:
    - Can we employ any remedial action?
    - What personal information has been affected?
    - Who may have had access to it?
    - What are the likely impacts?
4. Evaluate: the person or group needs to make a decision as to whether it is a notifiable data breach. This decision should be well documented, including the reasons why that decision was reached.

If an eligible data breach has occurred, the organisation must:-

1. Contain the breach in so far as it is possible,
2. Prepare a notification statement that contains:
    - the identity and contact details of the organisation
    - a description of the data breach,
    - the kinds of information affected, and
    - recommendations for affected individuals.
3. Provide a copy of the notification statement to the OAIC via the online form (www.forms.business.gov.au/smartforms/landing.htm?formCode=OAIC-NDB) or contact the OAIC enquiries line on 1300 363 992 to make alternative arrangements, and
4. Quickly notify individuals at likely risk of serious harm

6. Resources

1. Justice Connect – Not for Profit Law
2. Attachment one – flowchart prepared by The Office of the Australian Information Commissioner (OAIC)
3. Australian Privacy Principles under the Privacy Act 1988 (Cth),
4. Privacy Amendment (Notifiable Data Breaches) Act 2017 (NDB scheme)

7. Related documents

- Client Records Policy
- Feedback and Complaints Policy
- Mandatory COVID-19 Vaccination Policy
- HNS Cyber Security, Computer and Email Use