HPA Privacy Policy

Policy Statement

HPA Incorporated and its affiliates (HPA) is committed to protecting and upholding the right to privacy of participants, supported employees, staff, volunteers, trainees, students, Board members and representatives of agencies we deal with. HPA is subject to legislation applying to the organisation and its client group. The organisation will follow the guidelines of the Australian Privacy Principles in its information management practices.

For the purpose of this policy, clients, supported employees, staff, volunteers, carers, participants, Trainees, students Board members, Contractors and stakeholders shall be referred to as "Individual."

HPA will ensure:

- it meets its legal and ethical obligations as an employer and service provider in relation to protecting the privacy of individuals
- individuals are provided with information about their rights regarding privacy
- where possible individuals are provided with privacy when they are being interviewed or discussing matters of a personal or sensitive nature
- all individuals understand what is required in meeting these obligations.

This policy conforms to the Commonwealth Privacy Act (1988) and the 13 Privacy Principles which underpin the collection, use and storage of personal information.

This policy will apply to all records, whether hard copy or electronic, containing personal information about individuals, and interviews or discussions of a sensitive personal nature.

Australian Privacy Principles (APP)

APP 1 – Open and transparent management of personal information

HPA will take reasonable steps to implement practices, procedures and systems relating to our functions or activities that:

- complies with all the APP's
- is able to deal with inquiries or complaints from individuals about their compliance with APP's.

APP2 – Anonymity and pseudonymity

An individual can use services anonymously or under the name of an alias where lawful; however, HPA are unable to provide services for individuals under this AAP as our funding contracts require individuals to identify themselves appropriately.

APP 3 – Collection of solicited personal information

The most obvious method is collecting information directly from an individual such as through a form or initial assessment for services.

APP 4 – Dealing with unsolicited personal information

Receiving personal information pertaining to an individual which has not been sought. If this is the case the information should be destroyed or de identified.

APP 5 – Notification of the collection or personal information

At or before the time of collection of personal information HPA needs to take reasonable steps to inform the individual of the Collection Statement.

APP 6 – Use or disclosure of personal information

Holding of personal information about an individual that was collected for a particular purpose (Primary purpose), this information must not be used or disclosed for another purpose (secondary purpose) unless:

- consent has been sought to use the disclosure of the information
- one of the circumstances set out in APP 6.2 or 6.3 applies in relation to the use or disclosure of the information.

APP 7 – Direct marketing

Personal information may not be used or disclosed for direct marketing.

APP 8 – Cross border disclosure of personal information

Personal information may not be disclosed to a person overseas, as once the information has left Australia it is no longer has the protection afforded by the Privacy Act.

APP 9 – Adoption, use or disclosure of Government related identifiers

Identifiers such as Medicare or tax file numbers, DVA numbers cannot be used to identify an individual. HPA will adopt its own personal identifier number.

APP 10 – Quality of personal information

Information that is collected is accurate, complete, and up to date.

APP 11 – Security of personal information

Take reasonable steps to protect the information from misuse, interference, and loss from unauthorised access, modification, or disclosure.

APP 12 – Access to personal information

The Privacy Act provides individuals with the right to access their personal information – this applies to information collected after 21 DECEMBER 2001 and any information collected prior to that date which is still in use. An individual has the right to seek access to only their personal records.

APP 13 – Correction of personal information

An individual has the right to request a correction of their personal information if it is inaccurate, out of date, incomplete, irrelevant or misleading. HPA must take reasonable steps in the circumstances to correct the information.

Procedure

Dealing with Personal Information

In dealing with personal information, all HPA staff, carers, volunteers, and affiliates will:

- ensure privacy for individuals when they are being interviewed or discussing matters of a personal or sensitive nature
- only collect, use, and store personal information necessary for the functioning of the organisation, provision of service and other organisational activities
- use fair and lawful ways to collect personal information
- collect personal information only by consent from an individual
- ensure that individuals know what personal information is held, what purposes it is held it for and how it is collected, used, disclosed and who will have access to it
- ensure that where consent has been obtained, individuals are aware that consent may be withdrawn at any time
- 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 inaccurate information about themselves
- take reasonable steps to protect personal information from misuse and loss and from unauthorised access, modification or disclosure
- destroy or permanently de-identify personal information no longer needed and/or after legal requirements for retaining documents have expired.

Responsibilities for Managing Privacy

- All staff, carers, and volunteers of HPA are responsible for the management of personal information to which they have access. This includes information used for the conduct of research, consultation, or advocacy work.
- The Chief Executive Officer is responsible for content in HPA' publications, communications and website and must ensure that:
    - appropriate consent is obtained for the inclusion of any personal information about any individual including HPA personnel.
    - information being provided by other agencies or external individuals conforms to privacy principles.
    - the website contains a Privacy statement that makes clear the conditions of any collection of personal information from the public through their visit to the website.
- The Chief Executive Officer in conjunction with Management Committee members are responsible for overseeing safeguarding personal information relating to individuals.

Privacy contact officer shall:

- be appointed by the Chief Executive Officer and is the first point of contact when privacy issues arise either internally or externally
- ensure all staff are familiar with the Privacy Policy and administrative procedures for handling personal information
- ensure all staff and volunteers inform clients and other relevant individuals with information about their rights regarding privacy
- investigate queries or complaints about a privacy issue.

Privacy information for participants, students, and volunteers

Before or on entry to HPA services individuals will be given information on what is being collected, how their privacy will be protected and their rights in relation to this information.

Privacy for interviews and personal discussions

To ensure privacy for individuals when discussing sensitive or personal matters, the organisation will ensure that:

- information that is of a personal or sensitive nature is not discussed in public areas, including within HPA workplaces
- private interview space (where possible) for discussions with individuals and their advocates
- private spaces are provided for staff meetings that involve the discussion of participants
- private spaces will be sought for face to face or telephone discussions relating to individuals, where staff are required to discuss identifying or personal information in public areas, staff use non-identifying language to describe an individual or circumstance
- in instances where appointments with individuals are required outside of office opening hours, or in a person's home, every effort should be made to ensure that conversations are conducted in a private area.

Conduct Internal Privacy Audit and review of this policy

- HPA will conduct an internal audit of its process against the 13 APP. This will be a continuous process to ensure practices meet all the requirements of this policy.
- Compare current practices with the requirements of the 13 Australian Privacy Principles.
- As part of the internal audit process practices will be tested against the 13 APP's on a rotating process.
- Consult with stakeholders regarding organisational practices.
- Consultation with the Stakeholder Advisory Group will feed into the audit process and practices of the organisation.

Regular audit of the organisational complaints process

- Consultation with participants, supported employees, staff, volunteers and stakeholders will feed into the regular audit and continuous improvement of the complaints process.
- Inform clients, staff, volunteers, Management Committee members and contractors of the Privacy Policy and Complaints Procedure.
- All individuals will be given a copy of the Privacy Policy and information regarding the organisations Complaints Procedure.

Training of staff

- Induction of new individuals will be imbedded into induction and orientation.
- Regular re-training of existing staff (annually) to ensure all staff are up to date and have a working knowledge of this policy.
- Information staff are required to give to clients or participants of HPA:
    - Privacy Policy
    - Complaints information
    - Consent form.

Confidentiality of individuals records

HPA Incorporated utilises a cloud-based Client Management System eNDIS which is quality assured to ISO 27001. All information is stored within Australia.

Security

First layer

- Each staff member has a password to access the organisational electronic system.

Second layer

- Each Staff member has a username and password to access our CMS.
- Levels of access and authority within the system ensure staff can only access information relevant to their role and service.
- Footprint information can be reported on any part of the system.

Other

- Staff must ensure that they log off each time they leave their desk, equipment is set up to Sleep after a certain amount of time.
- Staff have access to only their individual passwords.
- Filing cabinets containing personal information is locked at the end of each day, and key stored securely.

All staff sign for any key usage

Staff asset register is kept ensuring tracking on data management equipment such as Laptops and mobile phones.

If staff are in a situation where they believe that they might have to divulge information about a participant or supported employee that they ordinarily would not disclose, they should seek the advice of their manager before making the decision to do so.

Organisational arrangements for maintaining individual's privacy and confidentiality will be reviewed on a tri-annual basis as part of a privacy audit, or sooner where an individual has a query on the privacy and confidentiality of their information.

Organisational internal privacy audit is an ongoing operational process. Any breaches in this policy will be addressed and changes made where appropriate.

Breaches of the Australian Privacy Principles

Individuals are within their rights under the Privacy Act to direct privacy related complaints to the organisation. Where possible, HPA should attempt to rectify the problem, and satisfy the complainant's request.

HPA have a procedure in place to ensure that all staff are well trained to facilitate this process.

HPA will ensure that all new staff are well trained in the policy and procedure, and all existing staff are notified when there are any changes or amendments to the procedure.

If the complainant is not happy with the response, then they may take their complaint to the Office of the Australian Information Commissioner.

If the complaint is upheld by the Office of the Australian Information Commissioner, the possible outcomes include: an apology, a change to the respondent's practices or procedures, staff training, or compensation for financial or non-financial loss.

If you want to make a complaint to us about how we have handled your private information, please put this in writing (please let us know if you need support to do this) to: COO@hpa.net.au

Process for correction of your personal and /or health information

You have the right to ask HPA to correct personal or health information. You can ask for this by contacting us – we must respond within 30 days.

This request must be made in writing (if you need support please let us know). HPA must take all reasonable steps to correct the information if considered it incorrect, unless there is a Law that allows or requires us not to

Process for access to your personal and /or health information

You have the right to ask HPA to have access to your personal and or health information. You will need to put your request in writing (if you need support please let us know). We must respond within 30 days of your request. You will be asked to verify your identity.

It may be appropriate or necessary for HPA to refuse individuals access to their records in certain circumstances, or restrict access to part of the records only, where providing access to the records would:

- be unlawful (refer to any relevant legislation in your jurisdiction)
- pose a serious and imminent threat to the mental health or life of an individual
- have an unreasonable impact on privacy of others (for example where services are
- provided to couples, families or groups)
- be frivolous or vexatious
- be prejudicial to an investigation or prosecution of alleged unlawful activity.

Once HPA receive your access request we will carefully review the records to consider the above. If HPA deny the above, we will notify you of the outcome and must provide our reasons in writing to you within 30 days.

Access Modes

HPA must provide access in the nominated method including:

- Together – HPA and individual go through the records/file and explain relevance.
- Verbally – HPA reads the records/file out to the individual and explain the relevance.
- Print copy – individual may have the records/file printed.
- A summary can be provided.

The Privacy Act allows for charges to be made in relation to access

- Photocopying fees – but not excessive.
- Fees for staff time to sit with individuals to read and go through records.
- Time to prepare for the access.
- HPA cannot charge individuals a fee for making the request.

Document Control

Document details	
Document title	HPA Privacy Policy
Policy reference and version	HR01
Date approved	8/04/2024
Statutory regulation	
Document review (e.g. annually)	2027

Change history			
Version	Date	Author	Change details
2.0	07/12/2023	Stephanie Ransome	Policy review
2.1	29/2/2024	Denise Watson	Minor formatting updates
2.2	8/4/2024	Denise Watson	Minor formatting update

Acronyms used in this document	
Acronyms	Full form
HPA	Helping People Achieve
APP	Australian Privacy Principles

Policy Approval

Approved by:
Kerry Whiting
Chief Executive Officer
HPA Incorporated

Signature

9/04/2024

Staff Signature			
Print Name			
Signature		Date	