Policy –	**Privacy Policy**		
Authorised by	Board of Directors (September 2023)		
Review Date	2023	Next Review Date	April 2025

1.0 Purpose

Bullinah Aboriginal Health Service (**BAHS**) uses all reasonable efforts to protect the privacy of individuals' personal information and to comply with the obligations imposed by the *Privacy Act 1988* (Cth) (**Privacy Act**) and the Australian Privacy Principles (**APP**).

We only collect personal information by lawful and fair means and only collect personal information that is necessary for our organisation's functions or activities.

If it is reasonable and practicable to do so, we collect personal information about an individual only from that individual.

We are transparent about the information we retain and the reasons for holding that information.

In meeting our obligations with respect to the privacy of our staff, clients, contractors and volunteers we acknowledge that people with vision or hearing impairments and those of culturally and linguistically diverse people may require special measures.

The purpose of this policy is to:

a) ensure personal information is managed in an open and transparent way;
b) protect the privacy of personal information of staff, clients, contractors and volunteers;
c) provide for the fair collection and handling of personal information;
d) ensure that personal information we collect is used and disclosed for relevant purposes only;
e) regulate the access to and correction of personal information; and
f) ensure the confidentiality of personal information through appropriate storage and security.

2.0 Scope

This policy applies to all current and future staff, contractors, clients, clients and volunteers.

3.0 Definitions

Personal Information	Personal Information is information or an opinion, 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.
Sensitive Information	Sensitive Information is a special category of Personal Information and includes information or an opinion about an individual's racial or ethnic origin, 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, criminal record, biometric information, biometric templates, health information about an individual and genetic information.
Unsolicited Information	Unsolicited Information is all Personal Information received from an individual that we did not actively seek to collect.
Health Information	Health Information is a record of: 1. information or an opinion about: a. the health including an illness, disability or injury (at any time) of an individual; b. an individual's expressed wishes about the future provision of health services to him or her; or

	c. a health service provided, or to be provided, to an individual that is also Personal Information; 2. other Personal Information collected to provide, or in providing, a health service; 3. other Personal Information about an individual collected in connection with the donation, or intended donation, by the individual of his or her body parts, organs or body substances; or 4. genetic information about an individual in a form that is, or could be, predictive of the health of the individual or a genetic relative of the individual.
Employee Record	An Employee Record is a record of Personal Information relating to the employment of an employee or former employee. Examples are Health Information about the employee and Personal Information about any of the following: a) the engagement, training, disciplining or resignation of the employee; b) the termination of the employment of the employee; c) the terms and conditions of employment of the employee; d) the employee's personal and emergency contact details; e) the employee's performance or conduct; f) the employee's hours of employment; g) the employee's salary or wages; h) the employee's membership of a professional or trade association; i) the employee's trade union membership; j) the employee's annual, long service, sick, personal, parental or other leave; and k) the employee's taxation, banking or superannuation affairs.
Record of registered tradesperson (contractors)	A record is held for tradespeople (contractors) registered to deliver services for BAHS. Examples of Personal Information relating to the tradesperson are: a) business registration b) qualifications c) insurance coverage d) invoices and payments

4.0 Policy detail

4.1 Collection

We collect and use information about you during the course of your relationship with us.

It is important that the information we hold about you is up to date. You must let us know when the information you have provided has changed.

4.1.1 Collection of personal information

We only collect Personal Information about an individual by fair and lawful means and only if the information is necessary for one or more of our functions as ahealthcare provider and collection of the Personal Information is necessary to:

a) comply with the provisions of state or commonwealth law;
b) provide data to government agencies in compliance with state or commonwealth law;
c) determine eligibility to entitlements provided under any state or commonwealth law;
d) provide appropriate services; and
e) lawfully liaise with a nominated representative and to contact family or next of kin if requested or needed.

Some individuals may not want to provide information to us. The information we request is relevant to providing them with the services they need. If the individual chooses not to provide us with some or all of the information we request, we may not be able to provide them with the services they require.

We do not collect your Sensitive Information unless the collection of the information is reasonably necessary for or directly related to one or more of our functions and:

a) you have consented to the collection of this information; or
b) the collection of the information is required by, authorised by or under an Australian law or a court/tribunal order; or
c) a permitted general situation exists to the collection of the information; or
d) a permitted health situation exists in relation to the collection of the information; or
e) we are a non-profit organisation and:
    a. the information relates to our activities; and
    b. the information relates only to the members of the organisation, or to individuals who have regular contact with us and our activities.

4.1.2 Methods of collection

Personal Information and Sensitive Information, may be collected:

a) from a prospective or staff member, client, contractor or volunteer;
b) from a related agency in regard to a client; and
c) from a legal advisor of a client.

We collect Personal Information directly from the client unless:

a) we have the consent of the client to collect the information from someone else; or
b) we are required or authorised by law to collect the information from someone else; or
c) it is unreasonable or impractical to do so.

A client should identify any parties from whom they do not wish Personal Information accessed or to whom they do not wish Personal Information provided. This should be recorded in the file of the client and complied with to the extent permitted by law.

4.1.3 Unsolicited Information

If we receive Personal Information from an individual that we have not solicited and we could not have obtained the information by lawful means, we will destroy or de-identify the information as soon as practicable and in accordance with the law.

4.1.4 Employee Records

We collect Personal Information about a staff member relating to their employment which forms part of their Employee Record (as defined above).

Our handling of Employee Records in relation to current and former employees is exempt from the Privacy Act and the APPs, where it directly relates to your current or former employment relationship. This means that you are not entitled to access your Employee Record.

4.1.5 Notification

At, or before, the time, or as soon as practicable after, we collect Personal Information from an individual, we take all reasonable steps to ensure that the individual is notified or made aware of:

a) our identity and contact details;
b) the purpose for which we are collecting Personal Information;
c) the identity of other entities or persons to whom we usually disclose Personal Information to;
d) that our privacy policy contains information about how the individual may complain about a breach of the APPs and how we will deal with a complaint;
e) whether we are likely to disclose Personal Information to overseas recipients and if so, the countries in which such recipients are likely to be located and if practicable, to specify those countries.

4.2 Use and disclosure of information

4.2.1 Collection of personal information

We may not use or disclose Personal Information for a purpose other than the primary purpose of collection, unless:

a) the secondary purpose is related to the primary purpose (and if Sensitive Information, directly related) and the individual would reasonably expect disclosure of the information for the secondary purpose;
b) the individual has consented;
c) the information is Health Information and the collection, use or disclosure is necessary for research, the compilation or analysis of statistics, relevant to public health or public safety, it is impractical to obtain consent, the use or disclosure is conducted within the privacy principles and guidelines and we reasonably believe that the recipient will not disclose the Health Information;
d) we believe on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to an individual's life, health or safety or a serious threat to public health or public safety;
e) we have reason to suspect unlawful activity and use or disclose the Personal Information as part of our investigation of the matter or in reporting our concerns to relevant persons or authorities;
f) we reasonably believe that the use or disclosure is reasonably necessary to allow an enforcement body to enforce laws, protect the public revenue, prevent seriously improper conduct or prepare or conduct legal proceedings; or
g) the use or disclosure is otherwise required or authorised by law.

If we receive Personal Information from an individual that we have not solicited, we will, if it is lawful and reasonable to do so, destroy or de-identify the information as soon as practicable.

4.2.2 Cross border disclosure

We do not disclose an individual's Personal Information to an overseas recipient. If we do, we will take all steps that are reasonable in the circumstances to ensure that the overseas recipient does not breach the APPs, unless:

a) the overseas recipient is subject to laws similar to the APPs and the individual has mechanisms to take action against the overseas recipient;
b) we reasonably believe the disclosure is necessary or authorised by Australian Law; or
c) the individual has provided express consent to the disclosure.

4.3 Access

You have a right to request that we provide you access to the Personal Information except for Employee Records, we hold about you, (and we shall make all reasonable attempts to grant that access) unless providing access:

a) is frivolous or vexatious;
b) poses a serious threat to the life or health of any individual;
c) unreasonably impacts upon the privacy of other individuals;
d) jeopardises existing or anticipated legal proceedings;
e) prejudices negotiations between the individual and us;
f) is unlawful or would be likely to prejudice an investigation of possible unlawful activity;
g) an enforcement body performing a lawful security function asks us not to provide access to the information; or
h) giving access would reveal information we hold about a commercially sensitive decision-making process.

4.3.1 Requesting access

Requests for access to information can be made orally or in writing and addressed to the Chief Executive Officer. We will respond to each request within 14 days.

4.3.2 Declining access

An individual's identity must be established prior to allowing access to the requested information. If unsatisfied with the individual's identity or access is requested from an unauthorised party, we can decline access to the information.

We can also decline access to information if:

a) there is a serious threat to life or health of any individual;
b) the privacy of others may be affected;
c) the request is frivolous or vexatious;
d) the information relates to existing or anticipated legal proceedings; or
e) the access would be unlawful.

We will provide in writing the reasons for declining access to the requested information.

4.3.3 Granting access

On request (and after determining an individual's right to access the information) we will provide access to Personal Information.

4.3.4 Charges

If we charge for providing access to Personal Information, those charges will not be excessive.

4.4 Personal information quality

We aim to ensure that the Personal Information we hold is accurate, complete and up-to-date. Please contact us if any of the Personal Information you have provided to us has changed. Please also contact us if you believe that the information we have about you is not accurate, complete or up-to-date.

4.5 Correction

If an individual establishes the Personal Information held about them is inaccurate, incomplete, out-of-date, irrelevant or misleading we will take reasonable steps to correct the information.

If we disagree with an individual about whether information is accurate, complete and up- to-date, and the individual asks us to add to the information, a statement claiming that the information is inaccurate, incomplete, out-of-date, irrelevant or misleading we will take reasonable steps to do so if deemed appropriate.

If we refuse to correct the Personal Information as requested by the individual, we will give the individual written notice that sets out:

a) the reasons for the refusal, except to the extent that it would be unreasonable to refuse;
b) the mechanisms available to complain about the refusal; and
c) any other matter prescribed by the regulations.

4.6 Direct marketing

4.6.1 Personal Information

We will not use or disclose Personal Information about an individual for the purposes of direct marketing, unless the information is collected directly from you and:

a) you would reasonably expect us to use or disclose your Personal Information for the purpose of direct marketing; and

b) we have provided you a means to 'opt-out' and you have not opted out.

4.6.2 Sensitive Information

We will not use or disclose Sensitive Information about an individual for the purposes of direct marketing, unless the individual has consented to the information being used for direct marketing.

4.6.3 An individual's rights in relation to direct marketing activities

If we use information for the purposes of direct marketing, the individual may:

a) ask us not to provide direct marketing communications;
b) ask us not to disclose or use the information; or
c) ask us to provide the source of the information.

4.7 Personal Information Security

We are committed to keeping secure the Personal Information you provide to us. We will take all reasonable steps to ensure the Personal Information we hold is protected from misuse, interference, loss, from unauthorised access, modification or disclosure.

4.8 Information of a Staff Member, Client, Contractors or Volunteer

a) We keep the records of a staff member, client or volunteer in a secure storage area.
b) Records of previous staff members, clients or volunteers shall be archived and stored in a locked service away from general use.
c) All records shall only be used for the purpose it was intended.
d) A staff member, client, contactor or volunteer, or their representatives shall be provided access to records relating to them, as requested and after consultation with the Chief Executive Officer. At these times, a qualified staff member is to remain with a staff member, client, contractor or volunteer or representative to facilitate the answering of questions raised.
e) Details of a staff member, client, contractor or volunteer are not to be provided over the phone, unless the staff member is sure of the person making the inquiry. If in doubt, consult the Chief Executive Officer.

4.9 Security measures

Our security measures include, but are not limited to:

a) training our staff on their obligations with respect to your Personal Information;
b) use of passwords when accessing our data storage system;
c) the use of firewalls and virus scanning tools to protect against unauthorised interference and access

We will, as soon as practicable and in accordance with the law, destroy or de-identify any Personal Information that is no longer required for our functions.

4.10 Data Breach

A data breach happens when Personal Information is accessed or disclosed without authorisation or is lost. If this occurs, we will notify affected individuals immediately and include recommendations about the steps to be taken in response to the data breach.

If a data breach involving Personal Information includes:

- unauthorised access to or unauthorised disclosure of Personal Information, or a loss of Personal Information, that we hold; and
- this is likely to result in serious harm to one or more individuals, and
- we haven't been able to prevent the likely risk of serious harm with remedial action,

we will notify the Office of the Australian Information Commissioner (**OAIC**) via the online Notifiable Data Breach Form.

4.11 Media

No member of staff shall make any statement to the press, radio or television station or to any reporter for the media. If a staff member is approached to make a statement or comment they must refer the person to our Chief Executive Officer.

5.0 Grievance procedure

5.1 Making a complaint

If you wish to make a complaint about the way we have managed your Personal Information you may make that complaint verbally or in writing by setting out the details of your complaint to the:

Chief Executive Officer / Privacy Officer
Phone: 0400676624
Email: CEO@bullinahahs.org.au

Alternatively, complaints may also be referred to the services as set out below:

Australian Information Commissioner: The Australian Information Commissioner receives complaints under the Act. Complaints can be made online http://www.oaic.gov.au/privacy/making-a-privacy-complaint; or by phone (1300 363 992); or in writing to one of the addresses below:

Office of the Australian Information Commissioner
GPO Box 5218
Sydney NSW 2001

OR

Office of the Australian Information Commissioner
GPO Box 2999
Canberra ACT 2601 NSW 2001

5.2 How we will deal with your complaint

The complaint will be investigated by us in accordance with our internal procedures and processes.

You may be invited to participate in a conference by the staff member conducting the investigation. At the discretion of the Chief Executive Officer, other interested parties may also be invited to participate in the conference to discuss the nature of the complaint and attempt to resolve it. This may include the presence or participation of a support person or advocate for the complainant.

You will be provided with a response to your complaint within a reasonable timeframe after completion of any investigation. This response will be in writing and will include the outcome of the investigation, any proposed action and details of the right to lodge a complaint with any relevant external organisations.

5.3 Privacy Officer

We have appointed a Privacy Officer to manage and administer all matters relating to protecting the privacy of individual's Personal Information.

The Privacy Officer can be contacted if any relevant person wishes to obtain more information about any aspect of this policy or about the way in which we operate to protect the privacy of individual's Personal Information.

As stated above, complaints may also be made to the Privacy Office if any person suspects we have breached this Privacy Policy, the Australian Privacy Principles or they are otherwise unhappy with the management of their or if they are responsible for another person, that person's Personal Information.