PRIVACY AND CONFIDENTIALITY POLICY

Date adopted: 14/03/2025		
Document Owner: Senior Leadership Team		
Authorised by: Senior Leadership Team		
Date last reviewed: 04/06/2021	Date of Current Review: 18/02/2025	Date of next review: 18/02/2028

Policy context: This policy relates to:	
Primary Policy or Framework	Governance Policy
Aged Care Quality Standards	1.2 Dignity, Respect and Privacy 2.7 Information Management
NDIS Practice Framework	NDIS Practice Standards and Quality Indicators [Core Module]
Legislation or other requirements	• *Aged Care Act* 1997 (Cth) • *Aged Care and Other Legislation Amendment (Royal Commission Response) Act* 2022 (Cth) • *National Disability Insurance Scheme Act* 2013 (Cth) • *Privacy Act* 1988 (Cth) • *Privacy Regulation* 2013 *(Cth)* • Australian Privacy Principles • Records Principles 2014 • Quality of Care Principles 2014 • *Privacy Amendment (Enhancing Privacy Protection) Act* 2012 (Cth) • *Privacy Amendment (Notifiable Data Breaches) Act* 2017 (Cth) • *Criminal Code Act* 1899 (QLD) • *Transport Operations (Passenger Transport) Regulation* 2018 (QLD) • *Fair Work Act* 2009 (Cth)
Related Internal Documents	• Charter of Aged Care Rights • Confidentiality Agreement • Code of Conduct Agreement • Misconduct Policy • Records Management Policy • Compliments and Complaints Management Policy • Client Incident Management Policy

	• Workplace Incident Management Policy • Health Photo Image Consent Form • Media Photo General Consent Form (General Release Form for All Media Projects) • Visual Consent Form (Respite) • Records and Information Management Policy

CONTENTS

Privacy and Confidentiality Policy 1

1. POLICY STATEMENT 4

2. PURPOSE 4

3. DEFINITIONS 4

4. PROCEDURES 5

4.1 Collection of Personal Information 5

4.2 Use and Disclosure of Personal Information 8

4.3 Security and Personal Information 9

4.4 Confidentiality Agreements 9

4.5 Access to Personal Information 10

4.6 Quality and Correction of Personal Information 10

4.7 Notifiable Data Breaches Scheme 10

4.8 Security Cameras 11

4.9 Employment Records and Employee Personal Information 12

4.10 Privacy Complaints 12

5. TRAINING AND COMPETENCIES 13

6. CONTINUOUS IMPROVEMENT 13

7. REVIEW & MONITORING 13

1. POLICY STATEMENT

Burnie Brae Ltd recognises the importance of privacy, security and confidentiality of information held about its clients, members, employees, volunteers, business partners and other individuals.

Burnie Brae Ltd is committed to managing personal and sensitive information in accordance with the requirements set out under the Australian Privacy Principles and the Privacy Act 1988.

2. PURPOSE

1. To ensure Burnie Brae meets its legislative and ethical obligations as an employer and service provider in relation to protecting the privacy of individuals through its systems, practices and procedures.

2. To ensure individuals are provided with information about their rights regarding privacy, including their right to access and correct their information, lodge a privacy complaint and have that complaint dealt with fairly and promptly.

3. To ensure all employees, board members, consultants, contractors, students and volunteers understand their responsibilities in relation to compliance with the Privacy Act and the Australian Privacy Principles.

3. DEFINITIONS

Throughout this policy, the following definitions apply:

Workers
Any person who carries out work in any capacity for Burnie Brae including:

- Employees
- Contractors
- Employee of a contractor
- Students
- Volunteers
- Board members

Client
Any individual who receives services from either Burnie Brae for the purpose of this policy, the term 'client' is inclusive of the terms client, consumer, participant, customer and member.

Australian Privacy Principles (APPs)
13 Principles formed as part of the Privacy Amendment (Enhancing Privacy Protection) Act 2012 which govern the standards, rights and obligations for:

- The collection, use and disclosure of personal information;

- Accountability and governance requirements in relation to personal and sensitive information;
- The integrity and correction of personal information held by Burnie Brae;
- The rights of individuals to access their personal information held by Burnie Brae.

Personal Information
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.

Health Information

- personal information about an individual that includes any of the following:
  - the individual's health at any time;
  - a disability of the individual at any time;
  - the individual's expressed wishes about the future provision of health services to the individual; or
  - a health service that has been provided, or will be provided, to the individual.
- personal information about the individual collected for the purpose of providing, or in providing, a health service; or
- personal information about the individual collected in connection with the donation, or intended donation, by the individual of any of the individual's body parts, organs or body substances.

Sensitive Information
Personal Information about an individual's:

- health;
- racial or ethnic origin;
- political opinions;
- membership of a political association, professional or trade association or trade union;
- religious beliefs or affiliations;
- philosophical beliefs;
- sexual orientation or practices;
- criminal record.

4. PROCEDURES

4.1 Collection of Personal Information

Collection of Personal Information
Burnie Brae collects Personal Information, and maintains records in order to:

- Communicate with clients;
- Provide services;
- Comply with reporting requirements to third parties, including government departments;

- To track our activities and operations.

Personal client information that Burnie Brae collects includes, but is not limited to:

- contact details for clients and their representatives or family members;
- details for emergency contacts and people authorised to act on behalf clients;
- clients' health status and medical records;
- medication records;
- service delivery intake, assessment, monitoring and review information;
- assessments, reviews and service delivery records;
- external agency information;
- feedback and complaints;
- incident reports; and
- consent forms.

Prior to collecting personal information from clients or their representatives, workers must explain:

- that Burnie Brae only collects personal information that is necessary for safe and effective service delivery;
- that personal information is only used for the purpose it is collected and is stored securely;
- what information is required;
- why the information is being collected and how it will be stored and used;
- the occasions when the information may need to be shared and who or where the information may be disclosed to;
- the client's right to decline providing information;
- the client's rights in terms of providing, accessing, updating and using personal information, and giving and withdrawing their consent; and
- the consequences (if any) if all or part of the information required is not provided.

Workers provide clients with a privacy statement as part of the Consumer Consent process at intake and during reviews.

Burnie Brae will, at all times, endeavour to only collect information needed to enable us to provide services to its clients, or to carry out a particular function or activity. Personal Information will be stored securely either in hard copy at our offices, or on secure data centres located in Australia.

Where possible, Burnie Brae will restrict access to Personal Information to individuals who have:

- a direct role in providing the service, function or activity;
- a quality assurance responsibility, i.e. auditing, supervision; or
- an administrative role related to records management.

Burnie Brae may collect Personal Information from third parties. This will only occur if:

- Burnie Brae reasonably believes the client would have expected the third party to have provided us with the information e.g. My Aged Care;

- Where the third party has told us that the client was informed about them providing us with the information;
- Where the client is informed that we are collecting the information from the third party.

When collecting Personal Information, workers are to ensure the client is informed of why we need the information and what we will do with it. We will endeavour to do this at the time of collection or, if not practicable, as soon as we can after collection.

At times it may be necessary for Burnie Brae to not disclose why the information is being collected. This may occur where it:

- May pose a serious threat to the life, health or safety of an individual, or pose a threat to public health or safety.
- May jeopardise the purpose of collection or the integrity of the Personal Information collected and there is a clear public interest in the purpose of collection.
- Would be inconsistent with another legal obligation, for example, by breaching a statutory secrecy provision, a client's legal professional privilege, or a legal obligation of confidence.
- Where the impracticability of notification, including the time and cost, outweighs the privacy benefit of notification.

Anonymity and Pseudonymity

Clients have the option to withhold personally-identifying information or to use a pseudonym when dealing with Burnie Brae. However, this only applies where it is reasonably practicable to do so and may limit the client from engaging in certain activities with Burnie Brae.

For example, clients are able to make an anonymous complaint, however, Burnie Brae will be unable to provide feedback to the client in relation to the complaint and the inability to contact the client for more information may limit the ability for the complaint to be fully investigated.

Passive Information Collection

Due to the use of various technologies, such as cookies, server logs and clickstream data, information can be passively collected by Burnie Brae, when navigating Burnie Brae websites. This means, that information can be gathered without the individual actively providing the information. For example, Burnie Brae may collect information about matters including, but not limited to, the date, time and duration of visits and which pages of a website are most commonly accessed. This information is generally not linked to an individual's identity, except where our website is accessed via links in an email.

Collection of Personal Information through websites, social media platforms and subscription services

Burnie Brae has a number of websites and social media platforms. Burnie Brae may collect Personal Information when:

- an email address is provided by an individual to subscribe to receive a newsletter or when signing up to activities, programs or events;

- an electronic/web form is completed. The information on completed electronic/web forms will be kept for as long as Burnie Brae requires the information to provide the service or information requested;
- an individual comments on a social media post;
- an individual leaves a review on a website or social media platform.

Burnie Brae newsletters and subscriptions will always provide a simple means for 'opting out' of receiving further updates and Burnie Brae will always comply with these requests.

Burnie Brae will not disclose personal information for the purpose of direct marketing unless the client has provided authorisation to do so.

Clients commenting on Social Media Platforms should be aware that any information posted or disclosed in these areas becomes public information and that Social Media Platforms have their own privacy policies relating to the handling of Personal Information.

Photos, Videos and Other Recordings

Photos, videos and other recordings are a form of personal information. This includes photos and videos taken for the purpose of service delivery and other purposes such as marketing and promotions. Workers must:

- ensure the collection, storage, use, storage, and disposal of photos, videos, and other recordings comply with the requirements of this policy and procedure;
- gain consent prior to taking a photo of any person any item belonging to that person:
    - For photos relating to hazards or incidents, verbal consent is acceptable, but must be documented in the incident report;
    - For photos of wounds, the 'Health Photo Image Consent Form must be completed and a copy saved to the client's file;
    - In Centre Day Respite, the Visual Consent Form must be signed and saved on the client's file.
    - For general media, the 'Media Photo General Consent Form (General Release Form for all Media Projects)' must be completed and a record kept.
- respect people's choices about being photographed or videoed or having their personal belongings or homes photographed or video recorded.
- ensure images or recordings of people are used appropriately and according to the person's wishes; and
- be aware of cultural sensitivities and the need for some images to be treated with special care.

4.2 Use and Disclosure of Personal Information

Use and Disclosure of Personal Information

1. No information is disclosed about an individual without their or their legal representative's consent except:
    - Non-identifying data required by funding bodies and by government departments for planning purposes.
    - Where disclosure is required or authorised by law (such as court subpoena or staff testifying under oath).

- Where it is reasonable to believe the disclosure is necessary to prevent or lessen serious threat to the life or health of the client or another person.
- To report missing persons.

2. Where information is disclosed, it is only used for the purpose for which it was intended.

Cross Border Disclosures

1. Burnie Brae will ensure no personal information is disclosed 'cross-border' to an overseas recipient until all reasonable steps have been taken to ensure no breaches relating to disclosure of personal information, will occur.
2. Only the CEO may authorise the transfer of personal information and only following receipt of individual consent.

Adoption, Use or Disclosure of Government Related Identifiers

Burnie Brae workers will not adopt, use or disclose a government related identifier unless an exception applies (please see Australian Privacy Principles for further information relating to exceptions).

4.3 Security and Personal Information

All Personal Information whether written, electronic, spoken or observed is to be treated as private and confidential.

Burnie Brae and its workers must take reasonable steps to protect the Personal Information it holds from misuse, loss, unauthorised access, modification or disclosure.

Minimal 'hard copy' Personal Information is kept, however, any 'hard copy' Personal Information is stored in key lockable filing cabinets or cupboards.

'Electronic information' is stored on secured data centres with security permissions applied to allow access to persons with authority to access the particular content. Burnie Brae have implemented frequent Information Technology (IT) health checks to ensure the safeguard of data and systems security.

Burnie Brae will safely destroy or delete Personal Information that is no longer required to be kept for authorised purposes. Further information about archiving and document and data retention can be found in the Records and Information Management Policy.

Documents are generally archived for 7 years prior to being safely destroyed, with the exception of the following types of records which are archived for 10 years prior to destruction –Work Health and Safety Records, IT records and health records, such as Healthy Connections and Allied Health records.

4.4 Confidentiality Agreements

All staff, volunteers, students and Board members agree to, and sign, a Confidentiality Agreement prior to be given access to any Personal Information.

All contractor agreements include clauses requiring contractors and their employees, to be bound by the Australian Privacy Principles and the Privacy Act.

4.5 Access to Personal Information

Clients have the right to request a copy or to view their Personal Information, including their client file, at any time:

1. All requests must be in writing and forwarded to the Manager of the associated program for actioning;
2. The Manager will consider all requests made by client or their requesting representative and should there be no eminent health risk to the client, information will be provided;
3. Should the Manager identify a risk to a client which may arise due to the disclosure of information from a client's file, this information may be withheld. Legal advice will be sought when required;
4. Burnie Brae reserves the right to invoice for the cost of providing a client file to clients and or their representatives, this does not include a cost to amend incorrect records on behalf of the client.

4.6 Quality and Correction of Personal Information

Burnie Brae makes every effort to ensure personal information collected is accurate, complete and up to date. This includes maintaining and updating Personal Information when we are advised that Personal Information has changed, is incorrect, out-of-date or misleading.

4.7 Notifiable Data Breaches Scheme

Under the Notifiable Data Breaches (NDB) scheme, Burnie Brae must notify affected individuals and the Office of the Australian Information Commissioner (OAIC) when a data breach is likely to result in serious harm to an individual whose personal information is involved.

A data breach occurs when personal information an organisation or agency holds is lost or subjected to unauthorised access or disclosure. For example, when:

- a device with a customer's personal information is lost or stolen;
- a database with personal information is hacked;
- personal information is mistakenly given to the wrong person.
- loss or theft of devices (such as phones, laptops, and storage devices) or paper records that contain personal information;
- unauthorised access to personal information by a staff member, for instance, a staff member browsing sensitive participant records without a legitimate purpose or a computer network being compromised by an external attacker resulting in personal information being accessed without authority;
- unauthorised disclosure of personal information due to 'human error', for example an email sent to the wrong person; and
- disclosure of an individual's personal information to a scammer, because of inadequate identity verification procedures.

Where a data breach is identified, response will be based on the following steps:
Step 1: Contain the data breach;
Step 2: Assess the data breach and the associated risks;
Step 3: Notify individuals and the Australian Information Commissioner; and
Step 4: Prevent future breaches.

Upon discovery of any identifiable personal information security breaches within Burnie Brae, the Chief Executive Officer (CEO) must be notified immediately by the Manager or Team Leader and an Incident Report will be completed.

The Head of Quality (or other delegated staff member) will investigate all breaches to establish if the breach is likely to result in serious harm to any individuals.

The Head of Quality will provide a report to the CEO within 3 business days, following notification of the breach with the following information:

- The type of breach (unauthorised access, unauthorised disclosure of personal information or loss of personal information).
- Whether the breach is likely to result in serious harm to one or more individuals.
- If the breach is unable to be contained, it is likely to result in a serious risk, even with remedial action.

The Head of Quality will consider the following information when investigating the type of breach and serious harm.

- Sensitivity of the information.
- Number of security measures protecting the information.
- Persons or kinds of persons who have obtained the information.
- Whether those persons could circumvent security technology.
- Nature of the harm.
- Other relevant considerations.

The CEO will review the investigation report and will decide whether the breach is considered a Notifiable Data Breach under the Notifiable Data Breaches Scheme.

If the breach is considered a Notifiable Data Breach, it will be reported to the ***Office of the Australian Information Commissioner*** and any affected parties, along with any corrective action within **30 days** from discovery of the breach.

4.8 Security Cameras

Burnie Brae uses security cameras in its buildings and vehicles in accordance with Australian and Queensland legislation.

This means that:

- Signage advising that CCTV cameras are in operation will be prominently displayed where use inside and outside of Burnie Brae buildings;
- Security cameras will only be used in public areas;

- Recorded personal information will be kept secure and destroyed when no longer required.

4.9 Employment Records and Employee Personal Information

Personal information held by Burnie Brae, relating to someone's current or former employment, isn't covered by the Australian Privacy Principles, if the information directly relates to the person's employment.

Burnie Brae maintains employee records and personal information (including volunteer records) as private and confidential and will not disclose an employee's personal information to any third party unless required:

- By a government agency or by law;
- By an auditor on behalf of a Government Department, the Aged Care Quality and Safety Commission or the NDIS Quality and Safeguards Commission;
- To fulfil the compliance requirements as a supplier to another Service Provider e.g. another Approved Provider may request police certificates for Burnie Brae staff providing services to their clients as part of a supply agreement.

Where possible, employee's permission will be requested prior to the disclosure.

Requests for employment records

If an employee, or former employee, requests access to their own employment records, Burnie Brae will make a copy available for them to inspect and copy. Alternatively, Burnie Brae will post a copy to the employee.

Providing References

Employees wishing to have a reference provided by Burnie Brae must ensure that the person providing the reference is aware of their consent to disclose their personal information relating to their employment.

Managers, supervisors and team leaders providing references are to only comment on facts relating to the employment relationship e.g. the employee's skills, performance and conduct, their type and length of employment. Sensitive information, such as medical information, should not be provided.

Unsuccessful Job Applicants

The Australian Privacy Principles do apply to personal information about unsuccessful job candidates. This includes applicants' resumes, contact details, references and academic transcripts. All personal information relating to unsuccessful job candidates will be destroyed within six months of the position being filled when the information is no longer required.

4.10 Privacy Complaints

Complaints about Privacy, including breaches of privacy and confidentiality, will be dealt with under the Compliments and Complaints Management Policy.
Privacy complaints can be made:

- By completing a Feedback form and handing it to a staff member or mailing the feedback form to the office;
- By email;
- By mail;
- By phone;
- In person;
- Online using the website feedback form.

Privacy Complaints can also be made to:

- The Office of the Australian Information Commissioner by:
  - completing an online privacy complaint form or
  - mailing GPO Box 5288, Sydney NSW 2001 or by
  - fax to +61 2 6123 5145.
- The NDIS Quality and Safeguards Commission;
- The Aged Care Quality and Safety Commission
- In writing to the Queensland Office of the Information Commissioner for complaints related to the privacy of health information:
  - Attention: Privacy Team
    Office of the Information Commissioner
    PO Box 10143
    Adelaide Street
    BRISBANE QLD 4001
  - Or Email: **administration@oic.qld.gov.au**
- To the Queensland Health Ombudsman for complaints about health services and health service providers, including registered and unregistered health practitioners: https://www.oho.qld.gov.au/make-a-complaint

5. TRAINING AND COMPETENCIES

All workers receive Privacy and Confidentiality training at induction and every three years, which includes how Personal Information is to be collected, used and disclosed in accordance with the Australian Privacy Principles and the Privacy Act.

6. CONTINUOUS IMPROVEMENT

Any Continuous Improvement actions identified relating to privacy, including actions resulting from Privacy Complaints and Data Breaches, will be included in the Continuous Improvement Register.

7. REVIEW & MONITORING

This policy will be reviewed every three years in consultation with managers and workers.