| Policy No. POL 05 | |
|---|---|
| **Privacy and Confidentiality** | PRESTIGE inhome care |

## Statement

Prestige Inhome Care (Prestige) is committed to protecting all personal information and ensuring that the handling of Personal Information provided by job seekers, staff, clients, volunteers and others with whom we deal complies with Australian Privacy laws. This includes Australian Privacy Principles (**APP**s) outlined in the Privacy Act 1988 (Commonwealth) (**Privacy Act**) and any applicable state or territory legislation.

Prestige upholds each individual's right to dignity, autonomy and privacy, including as reflected in the Aged Care Act 2024 Statement of Rights, and manage personal and health information in a manner that is respectful, secure and supports informed choice and control.

We also operate in accordance with the Strengthened Aged Care Quality Standards and the NDIS Practice Standards to ensure personal information is handled in a way that supports the delivery of safe, high-quality care and services.

This policy outlines how personal information is collected, used, disclosed, stored and managed in accordance with applicable privacy and related legislation.

## Legislative and Regulatory Requirements

This policy is aligned with:

- Aged Care Act 2024 (including the Statement of Rights and obligations relating to the delivery of high-quality care)
- Strengthened Aged Care Quality Standards
    - Standard 1: The Person
    - Standard 2: The Organisation
- National Disability Insurance Scheme Act 2013
- NDIS Practice Standards
- NDIS Code of Conduct
- Privacy and Information Laws
    - Privacy Act 1988 (Cth) (including Australian Privacy Principles)
    - Health Records Act 2001 (VIC)
    - Privacy and Data Protection Act 2014 (VIC)
    - Health Records and Information Privacy Act 2002 (NSW)
    - Information Privacy Act 2009 (QLD)
    - Spam Act 2003 (Cth
- Information sharing, Safeguarding and Mandatory reporting
    - NDIS Reportable Incidents and Complaints framework
    - Aged Care Serious Incidents Response Scheme (SIRS)
    - Notifiable Data Breaches Scheme

## Definitions

***Personal Information***

Information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not and whether the information or opinion is recorded in material form or not.

***Health Information***

- Information or an opinion about:
    - The health or a disability at any time of an individual;
    - An individual's expressed wishes about the future provision of health services to him/her;
    - A health service provided or to be provided to an individual that is also Personal Information;
- Other Personal Information collected to provide, or in providing a health service;
- Other Personal Information about an individual collected in connection with the donation, or intended donation by the individual of his/her body parts, organs or body substances;
- 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.

***Sensitive information*** - a subset of personal information and refers to information or an opinion about an individual's:

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

***Unsolicited Information***

Unsolicited Information is all Personal Information received from an individual that Prestige does not actively seek to collect.

***Employee Record***

An Employee Record is a record of Personal Information relating to the employment of a member of staff. Examples of Personal Information relating to the employment of the staff member may include:

- The engagement, training, disciplining or resignation of the employee;
- The terms and conditions of employment of the staff member;
- The employee's personal and emergency contact details;
- The employee's performance or conduct;
- The employee's criminal record status as obtained through a National police check or Working with Children Check;

## 1. Collection of personal Information

Prestige will only collect personal information that is reasonably necessary to deliver services, perform our functions and activities and comply with legal and regulatory obligations.

Personal information is collected to:

- Comply with applicable Commonwealth and State or Territory laws
- Meet reporting and information-sharing obligations with government agencies where required by law
- Deliver safe, personalised and high-quality care and supports
- Respond to enquiries and requests for services from individuals or their representatives
- Support communication with a person's nominated representative or support person, where authorised or consented to
- Engage and manage our workforce including employees, contractors or consultants

We collect and handle personal information in a manner that supports each individual's right to dignity, autonomy, privacy and informed decision-making, consistent with the Aged Care Act 2024 and the NDIS Practice Standards.

Types of information collected may include:

- Name, address and contact details (e.g. Phone and email).
- Payment and billing information (e.g. Credit Card or bank account details).
- Current medical history, past history and relevant Health Information including Treating Practitioners' name and contact details.
- Advance Care Planning documentation (where applicable)

We will only collect sensitive Information (including health information) where the information is reasonably necessary for or directly related to one or more of Prestige's functions and:

- The individual has provided informed consent.
- The collection is required or authorised by law.
- A permitted health situation exists in relation to the collection of the information
- The collection of information is a requirement for staff employment and/or business activities.

Individuals may choose not to provide personal information to Prestige. However, if sufficient information is not provided, we may be unable to deliver safe, appropriate and effective care and services.

Prestige collects information through a variety of ways including:

- Direct interactions (face to face, phone, email or digital platforms)
- Through our website;
- From third party referral services (with appropriate consent or authority)
- Through provision of care and services.

## 2. Use and Disclosure of Information

We will only use and disclose personal information for the primary purpose for which it was collected, or for a directly related secondary purpose that an individual would reasonably expect, in accordance with the Privacy Act 1988.

We may otherwise use or disclose personal information with the individual's consent or where required or authorised by law.

Personal information may be shared with government agencies, regulators and other providers where necessary to deliver safe, lawful and high-quality care and supports, and to meet our regulatory obligations under the Aged Care Act 2024 and the NDIS Practice Standards.

### 2.1 Communication and marketing

We will only use and disclose personal information for the primary purpose for which it was collected, or for a directly related secondary purpose that an individual would reasonably expect, in accordance with the Privacy Act 1988.

We will only send direct marketing communications where permitted under applicable privacy laws and the Spam Act 2003, and where the individual has provided consent or would reasonably expect to receive such communications.

Individuals may opt out of receiving marketing communications at any time using the unsubscribe option provided or by contacting us via email to feedback@prestigeinhomecare.com.au or call us directly on 1300 10 30 10.

### 2.2 Employee information

We may use and disclose personal information relating to employees and prospective employees for purposes including recruitment, verification of qualifications, reference checks and workforce management, in accordance with applicable laws

Personal information may be disclosed to third parties where reasonably necessary for these purposes, including educational institutions, referees, background screening providers and regulatory bodies.

We take reasonable steps to ensure employee personal information is accurate, secure and handled in a confidential manner.

### 2.3 Disclosure to third party service providers

We may disclose client Personal Information to third party contractors and service providers that help us to operate our business and to deliver services to clients, such as, without limitation, IT service providers, Allied Health providers, General Practitioners, Hospitals, payment system operators, financial institutions, debt collectors, couriers, accountants, solicitors, business advisors and referral services (including to enable the referral service to verify whether a client was referred to us by that service).

When Prestige provides Personal Information to companies who perform services on our behalf, we require those companies to protect Personal Information as diligently as we do. Strict contractual and other quality assurance measures are used to ensure Personal Information is protected.

This may include sharing information with other care providers and associated providers to support care coordination, continuity of care and service delivery.

### 2.4 Disclosure to advertisers

Prestige does not sell, rent or actively share clients' personal or health information for advertising or marketing purposes. We do not provide client care information to advertisers.

Like most websites, our website may use cookies and similar technologies provided by third-party platforms (such as search engines or social media services) to help us understand website usage and improve our online content. This may result in visitors seeing more relevant advertising from those platforms elsewhere online.

Any information collected through website cookies is limited, does not include health or care information, and is handled in accordance with our Privacy and Confidentiality obligations.

Visitors can manage or disable cookies through their browser settings and can contact us at feedback@prestigeinhomecare.com.au or 1300 10 30 10 if they have questions about how personal information is handled.

### 2.5 Disclosure to relatives and guardians

There are certain instances where Prestige may need to share or disclose an individual's Personal Health Information to an authorised representative, support person or person responsible the individual (i.e. a parent, child, sibling, relative, guardian or power of attorney). We may do so, in accordance with Health Privacy Principle 2, if:

- the individual is incapable of giving consent or communicating consent;
- Prestige Management or Coordination staff are satisfied that the disclosure is necessary to provide appropriate care or treatment, is made for compassionate reasons or for the purposes of undertaking a quality review of our services; or
- the disclosure is not contrary to any wish previously expressed by the individual which the organisation is aware of, or of which the organisation could reasonably be expected to be aware, and the disclosure is limited to the extent reasonable and necessary for providing care or treatment.

### 2.6 Disclosures required or permitted by law

We may use or disclose personal information where required or authorised by law, including for the purposes of responding to lawful requests from government agencies, courts or regulators, or where necessary to prevent a serious threat to life, health or safety, investigate unlawful activity or support law enforcement functions. For example:

- disclosure to various government departments and agencies such as the Australian Taxation Office, Centrelink, Child Support Agency, or disclosure to courts under subpoena; and
- disclosure permitted under Health Privacy Principle 2, where Prestige:
    - reasonably believes that 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;
    - has reason to suspect unlawful activity and uses or discloses the Personal Information as part of our investigation of the matter or in reporting our concerns to the relevant authorities;
    - reasonably believes 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.

## 3. Data Security

Prestige will take reasonable steps to protect Personal Information that we hold from misuse, interference, loss or unauthorised access, modification or disclosure.

**Security Measures**

Our security measures include, but are not limited to:

- implementing role-based access controls to ensure Personal Information is only accessed by authorised personnel where required for their role
- requiring secure authentication processes to access systems and information
- storing records in secure electronic systems with appropriate safeguards, including firewalls, virus protection and system monitoring
- maintaining physical security measures for devices, systems and any hard copy records
- training staff on privacy, confidentiality and information security obligations, including the protection of dignity and privacy
- requiring all staff to undergo appropriate screening and to comply with confidentiality obligations

**Contractors and Third Parties**

Contractors, subcontractors and other third parties (including associated providers) engaged by Prestige are required to:

- Comply with applicable Australian privacy laws and the Australian Privacy Principles
- Only access or use Personal Information where necessary to perform agreed services
- Maintain appropriate confidentiality and information security controls
- Ensure devices and systems used to access Personal Information are appropriately secured
- Notify Prestige immediately of any actual or potential breaches of security

**Overseas Disclosure**

In some circumstances, Personal Information may be stored in or accessed from overseas (for example, through secure cloud-based systems or service providers). Where this occurs, Prestige takes reasonable steps to ensure that overseas recipients handle Personal Information in a manner consistent with the Australian Privacy Principles or are otherwise subject to substantially similar privacy obligations.

**Information held in client's home**

Where Personal or health information is kept within a client's home as part of service delivery, Prestige takes reasonable steps to ensure that access is limited to authorised workers for the purpose of providing care. However, due to the nature of in-home services, Prestige acknowledges that access by others may occur and is not always within its control.

**Retention and disposal**

Prestige will take reasonable steps to destroy or de-identify Personal Information when it is no longer required for its functions or activities, unless the information is required to be retained under Australian law or for legitimate business or care-related purposes.

## 4. Cloud & AI Technology

Prestige aims to safeguard sensitive information, maintain trust with stakeholders, and comply with legal and regulatory requirements in the cloud and AI systems it uses to operate its business.

### 4.1 Data Classification

- All data used in Cloud and AI systems must be classified based on sensitivity and confidentiality level.
- Data classification should be conducted in accordance with company policies and relevant regulatory requirements.

### 4.2 Access Control

- Access to data used in Cloud and AI systems should be granted on a need-to-know basis.
- Role-based access controls should be implemented to restrict access to sensitive data.
- Access should be regularly reviewed and revoked when no longer necessary

### 4.3 Data encryption

- All data used in Cloud and AI systems, especially sensitive or personally identifiable information (PII), must be encrypted both in transit and at rest.
- Strong encryption algorithms and protocols should be used to protect data integrity and confidentiality.

### 4.4 Data Handling and Storage

- Data used in Cloud and AI systems should be stored in secure environments with appropriate safeguards against unauthorized access.
- Secure storage solutions, such as encrypted databases or cloud storage with strong access controls, should be utilised.
- Data should be retained only for as long as necessary, and disposal should be conducted securely in accordance with company policies

### 4.5 Data Processing

- Data processing for Cloud and AI purposes should be conducted in compliance with relevant laws and regulations, including data protection and privacy laws.

- Measures should be implemented to ensure that AI algorithms do not inadvertently expose sensitive information or violate user privacy.

**4.6 Training and Awareness**

- All employees involved in Cloud and AI development, deployment, or maintenance should receive training on data confidentiality best practices and compliance requirements.
- Regular awareness programs should be conducted to reinforce the importance of data confidentiality and promote a culture of security within the organisation.

**4.7 Third party vendors**

- Third-party vendors providing Cloud and AI-related services or solutions must adhere to the same data confidentiality standards as Prestige
- Contracts with third-party vendors should include provisions for data protection and confidentiality, as well as mechanisms for auditing their compliance.

**4.8 Monitoring and Enforcement**

- Regular audits and monitoring should be conducted to ensure compliance with this policy.

## 5. Access or changes to Personal Information

Prestige takes reasonable steps to ensure that the Personal Information it holds is accurate, complete and up to date.

You may request access to the Personal Information we hold about you, and request correction of that information if you believe it is inaccurate, out of date, incomplete, irrelevant or misleading.

In accordance with the Privacy Act 1988 (Cth) and the Health Records Act 2001 (VIC), we may decline a request for access in certain circumstances, including where:

- providing access would have an unreasonable impact on the privacy of other individuals
- the request is frivolous or vexatious
- the information relates to existing or anticipated legal proceedings
- denying access is otherwise required or authorised by law

If we refuse access or correction, we will provide written reasons, except where it would be unreasonable to do so.

If we do not agree that there are grounds for amendment, then we will add a note to the personal information stating that you disagree with it.

We will take reasonable steps to verify your identity and authority before granting access to or making changes to Personal Information, including where a request is made by an authorised representative.

## 6. Notification

When we collect Personal Information directly from an individual, we will take all reasonable steps to ensure that they are aware of the collection of their Personal Information.
If information is collected from a 3rd party, reasonable steps will be taken to notify the individual or otherwise ensure that the individual is aware that the information will, or may be, passed on to us.

## 7. Data Breaches

Under the **Notifiable Data Breaches Scheme** (Part IIIC of the Privacy Act 1988), Prestige have an obligation to notify affected individuals and the Office of the Australian Information Commissioner (OAIC) about an eligible data breach which is likely to cause serious harm to any of the individuals to whom the information relates.

In the event of a data breach, Prestige will:

- investigate suspected security incidents to determine if an eligible data breach has occurred so that it can be reported;
- assess the risk of serious harm to affected individuals if personal information is disclosed or lost;
- notify affected individuals and the OAIC where applicable;
- review any contracts with third parties who hold personal information on behalf of the entity and ensure that adequate contractual provisions are in place to manage compliance with the notification regime;

- Record the data breach in our Incident Management Database to ensure a record is maintained of how the breach or suspected breach was managed.

### 7.1 Data Breach Notification Obligations

- In the event of an eligible data breach, Prestige is required to notify the Office of the Australian Information Commissioner (OAIC) using the online Notifiable Data Breach Statement Form and affected individuals as soon as practicable after becoming aware that there are reasonable grounds to believe that there has been an eligible data breach.
- If Prestige has taken remedial actions and steps to address any potential harm to individuals to whom the information relates before any serious harm is caused, there is no mandatory obligation to report the data breach. The incident should still be recorded in Risk Wizard as documented evidence of the remedial actions and steps taken to mitigate any serious harm.

## 8. Making a Complaint (Grievance Procedure)

Privacy Law is regulated by the Australian Information Commissioner. Further information about privacy legislation can be obtained from the Office of the Australian Information Commissioner website at www.oaic.gov.au

Prestige takes all complaints seriously. Anyone who wishes to make a complaint about the way Prestige Inhome Care has managed their Personal Information may make that complaint verbally or in writing by setting out the details of the complaint to any of the following:

- Prestige Inhome Care Privacy Officer,
  Phone: 1300 10 30 10
  Email: privacy@prestigeinhomecare.com.au
- Office of the Australian Information Commissioner.
  - Online: http://www.oaic.gov.au/privacy/making-a-privacy-complaint
  - By phone: 1300 363 992
  - In writing to Office of the Australian Information Commissioner
    GPO Box 5218, Sydney NSW 2001

## 9. Review and Improvement

Prestige may update this policy from time to time to reflect changes in legislation or internal process changes. An up-to-date copy of this policy will be maintained on the Prestige website at all times https://www.prestigeinhomecare.com.au/feedback-privacy-policy/.

## 10. Policy violation

Violations of data confidentiality policies should be promptly investigated and appropriate disciplinary action taken, which may include termination of employment or contract.

**Related Documents**
POL 45 Information Technology Policy
PRO 45 F1 Data Breach Response Plan
POL 36 Record Management Policy
PRO 07 F13 Guardianship and Administration
PRO 07 F29 Advance Care Directive - Statement of Choices