


Policy No. POL 05	
Privacy and Confidentiality	

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 (**APPs**) outlined in the Privacy Act 1988 (Commonwealth) (**Privacy Act**) and any applicable state or territory legislation.

This policy outlines how we collect, use, disclose, store and manage personal information in accordance with these Australian Privacy Laws.

Legislation

Prestige will manage all personal information in accordance with Australian Privacy laws including (but not limited to):

- Privacy Act 1988 (Cth), and the Australian Privacy Principles (APPs)
- Freedom of Information Act 1982
- Spam Act 2003
- Privacy and Data Protection Act 2014 (Vic)
- Privacy and Personal Information Protection Act 1998 (NSW)
- Health Records and Information Privacy Act 2002 (NSW)
- Health Records Act 2001 (Vic), including the Health Privacy Principles
- Charter of Human Rights and Responsibilities Act 2006 (Vic)
- Information Privacy Act 2000 (Vic)
- The Information Privacy Act 2009 (QLD)
- Right to Information Act 2009 (QLD)

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.

Policy No. POL 05	
Privacy and Confidentiality	

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 necessary to deliver our services and conduct the business activities that support this and where the collection of the personal information is necessary to: .

- Comply with the provisions of State or Commonwealth laws
- Provide data to Government agencies as required by State or Commonwealth law
- Provide appropriate services and care to our clients
- Respond to requests for services from potential clients or their representatives
- Enable contact with a nominated person regarding an individual's health status
- Lawfully liaise with a nominated representative and to contact family/representatives as requested or needed
- Engage with current or prospective staff, contractors or consultants

All employees have been screened and have signed a confidentiality agreement, which ensures Personal Information to which they may become exposed to through the course of their employment, remains confidential.

The type of information that we collect includes, but is not limited to:

- Your name, address and contact details (e.g. Phone and email);
- Payment details (e.g. Credit Card or bank account details);
- Your current medical history, past history and relevant Health Information including Treating Practitioners' name and contact details;
- Advance Care Directive


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 consented to the collection of this information
- The collection of the information is authorised under an Australian law or a court/tribunal order
- 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.

Some individuals may not want to provide information to Prestige. If the individual chooses not to provide some or all of the information requested, Prestige may as a result be unable to provide them with the care and services they require.

Prestige collects information through a variety of ways including:

- Electronic or face to face interactions;
- Through our website;
- Requests for information;
- From third party referral services; and
- Through provision of services.

Policy No. POL 05	
Privacy and Confidentiality	

2. Use and Disclosure of Information

Generally, we will only use and disclose Personal Information for purposes consistent with the reason this information was collected or for a directly related purpose, unless we have the individual's express or implied consent to use or disclose it for a different purpose.

Prestige may disclose personal information without your consent if required or authorised to do so by law.

2.1 Communication and marketing

We may use personal information to communicate with individuals through emails, newsletters or direct marketing, in accordance with Privacy legislation and the Privacy Act, unless the individual has previously requested that we do not do so. All such communication will provide the option to opt out or unsubscribe. A request to opt out or unsubscribe can also be sent directly to feedback@prestigeinhomecare.com.au or call us on 1300 10 30 10.

2.2 Employee information

We may use/disclose employees' or prospective employees' personal information, with consent, to:

- obtain references from former employers or give references to potential employers;
- verify qualifications with educational or vocational organisations;
- conduct background and criminal records checks (provided that the organisation complies with privacy laws).

Some Personal information may be shared with clients, their family members/guardians and/or their authorised representatives for the purposes of service provision;

Personal information may be shared for the purpose of service provision, performance management and general operations;

Personal information may be shared as part of mandatory inspections or investigations by the ATO, Fair Work, WorkSafe/SafeWork, police, government departments (e.g. Department of Health), Commissions or their delegates.

When dealing with employee personal information, Prestige will endeavour to:

- Limit the collection of information
- Provide notice to individuals about the potential collection, use and disclosure of personal information
- Keep employee's personal information accurate, complete and up to date
- Keep employee's personal information secure
- Provide employees access to their personal information

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.

2.4 Disclosure to advertisers

Prestige Inhome Care partners with third party ad servers, ad networks and social media platforms (like Facebook and Google) to deliver personalised advertisements on our service that may be of interest to you and/or to measure their effectiveness, and/or to identify potential new users of our service.

We may share certain information with our third party advertising partners, such as your email address, location, cookie information and information relating to your use of our service, and allow partners to perform a match of your information against information from other third party networks or sites to serve ads either on the service or on third party sites (including, but not limited to Facebook and Google) and to measure the effectiveness of these ads. We also share certain information with social media platforms, such as Facebook,

Policy No. POL 05	
Privacy and Confidentiality	

to display advertising to potential new users whose demographics and behaviour look like those of our existing users.

Prestige Inhome Care does not sell or rent the information we collect directly from you or about you from third parties with these third-party ad servers or ad networks for such parties' own marketing purposes.

You can opt out of having your email matched or shared with third party advertising partners by emailing feedback@prestigeinhomecare.com.au or calling 1300 10 30 10.

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 a person who is responsible for 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

In some circumstances we are authorised or required by law to disclose certain personal information. 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 does not store any of your confidential material overseas. If we do, we will take all reasonable steps to ensure the overseas recipient does not breach the Australian Privacy Principles or the overseas recipient is subject to laws similar to the Australian Privacy Principles.


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

Our security measures include, but are not limited to:

- Training our staff on their obligations with respect to your personal information and ensuring they protect and respect your privacy, dignity and confidentiality at all times.
- Client and staff records are stored electronically and use of passwords is required when accessing our data storage systems
- Use of firewalls and virus scanning tools to protect against unauthorised interference and access

Contractors working on behalf of Prestige are required to:

- Comply with all Australian privacy laws and the Australian Privacy Principles
- Have up to date software protection installed on any device used to access or store personal information
- Notify Prestige immediately of any actual or potential breaches of security

Policy No. POL 05	
Privacy and Confidentiality	

Personal and Health Information may also be held within a client's home as part of their health care record. While Prestige endeavours to ensure this is only accessed by employees in order to provide appropriate care, it is acknowledged that access by others is possible and is outside of the control of Prestige.

We will, in accordance with the law, destroy or deidentify and personal information that is no longer required for our functions

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

Policy No. POL 05	
Privacy and Confidentiality	

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

5. Access or changes to Personal Information

We endeavour to ensure that the personal information we hold is accurate, complete and up to date.

Individuals may request access to their own Personal Information kept by Prestige and have a right to advise us of any perceived inaccuracy. Where reasonable and practical to do so, and in accordance with the provisions of the Privacy Act and Health Records Act, Prestige will provide access to an individual's personal information.

There may be instances where we cannot grant you access to the Personal Information or Health Information we hold. For example, we will refuse access if granting access would interfere with the privacy of others or 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 the personal information we hold about you is incorrect, incomplete or inaccurate, then you can request us to amend it. We will consider if the information requires amendment. 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.

In all cases, Prestige must be satisfied access to/or changes to information are authorised by the individual in question.

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)

Policy No. POL 05	
Privacy and Confidentiality	

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