

05: Privacy

---

## 1. Policy Statement

Providing All Living Supports (PALS) Inc. is committed to maintaining a person’s right to privacy by upholding the Australian Privacy Principles (APP) and complying with the Privacy Act 1988 (Cth) and other relevant regulations, legislation and contractual requirements.

Although the Privacy Act does not apply to employee records being used for employment related purposes, PALS will endeavour to follow best practice as guided by the Australian Privacy Principles.

PALS collect personal and sensitive information:

- with the prior knowledge and consent of the person (or their legal representative);
- in a fair, non-intrusive and lawful way;
- only if necessary for the function of the service or organisation;
- without intrusion into areas of a person’s life that are irrelevant to the services provided;
- directly from the person, where practical and appropriate, rather than a third party;
- after informing the person why the information is being collected and how it will be used; and,
- in an environment where confidentiality can be maintained.

PALS ensures the effective storage, backup, retrieval, archiving and retention of electronic and printed organisational data, to maintain business continuity and compliance with privacy and record retention obligations and other relevant regulations, legislation and contractual requirements including mitigation and notification obligations where a privacy breach occurs.

PALS considers privacy breaches can have serious consequences and have robust systems and procedures in place to identify and respond effectively when a breach is identified.

## 2. Purpose

This policy outlines the rights and responsibilities regarding the collection, handling, security, retention, accuracy, and access to personal, sensitive, and confidential information.

## 3. Scope

This policy applies to the following:

Employees	Directors	Clients	Contractors (including employees of contractors)	Volunteers	Suppliers	Consultants
✓	✓	✓	✓	✓	✓	✓

Within this policy, all these people, except clients, are represented by the term “Workers”.

## 4. Definitions

Term	Meaning
Employee records:	Records kept by PALS relating to the employment of a staff member.
Personal information:	Refers to information or an opinion that identifies an individual. This may include a person's name, address, photograph, contact details, date of birth, employment details or any information where the person is reasonably identifiable.
Sensitive information:	Is a subset of personal information and may include a person's cultural or ethnic origin, health information (such as disability or use of health services), religious beliefs, political opinions, sexual orientation, or criminal record.
Confidential information:	Refers to other information that PALS informs employees is to be kept private or could reasonably be assumed to be. This may include organisational financial and governance information, pending tender applications, employee information and records and the intellectual property of the organisation.

## 5. Policy

### 5.1 Collection of Information

PALS collect and hold information which is reasonably necessary for the organisation to conduct its usual activities and operations, including developing and delivering services, evaluating outcomes, sharing stories through marketing and conducting research. The kind of information collected and held includes (but is not limited to) personal information about participants, service users, students, volunteers, directors, contractors and providers.

When interacting with PALS, a person can choose to be anonymous or use a pseudonym, except where it is required or authorised by law to deal with identified individuals, or it is impracticable to deal with individuals who have not identified themselves.

If we do not collect necessary personal information, we may not be able to provide support or services to participants, service users, employees, contractors and providers.

#### 5.1.1 The kinds of personal information collected

The types of personal information that PALS collect includes:

- name, contact details, date of birth and age;
- gender, details about participants physical and mental health, including disabilities;

## 05: Privacy

---

- information about participant's support requirements, including details of family and other relationships;
- details of feedback or complaints about services provided by us;
- details of interactions, including any contact we have in person, by email, online or on the telephone;
- images of people in photographs or film;
- bank account details; and,
- employee records.

### 5.1.2 How is personal information collected and stored

PALS may collect information in a number of circumstances, including when a person:

- is required to provide consent to engage with PALS in a service, activity or event;
- provides feedback or requests information from PALS;
- applies for a job, work placement or volunteer position;
- makes a donation; or
- joins a mailing or contact list.

PALS often collect personal information from people directly, or from people who are authorised to represent them. Personal information is held securely electronically (and may include hard copy form at PALS offices).

Sometimes, personal information is collected from a third party if the person has consented, been told of this practice, or would reasonably expect PALS to collect the information in this way. Examples of this include, but are not limited to, collecting information from:

- a healthcare service that manages a participant's care.
- internet service providers for the purposes of targeted marketing initiatives.

PALS will seek consent before taking photographs and recordings of individuals using or participating in our services, programs or facilities and before publishing information that identifies an individual in any printed, electronic, video or audio publications.

Personal information is collected about employees and prospective employees in order to conduct employment and employment-related activities such as payroll services, recruitment and selection, performance management, reporting and work health and safety.

PALS uses third-party systems to store some of our data, such as HR management and client management systems. Where this occurs, PALS has a service agreement with these third parties which incorporates our Privacy Policy, Privacy Principles, and the Privacy Act.

### 5.1.3 How is personal information kept secure

Personal information is kept in a manner that reasonably protects it from misuse, loss, unauthorised access, modification or disclosure. This includes keeping hard copy information in locked cabinets with restricted access and using security controls for electronic information that include authorised access, user authentication, email filtering, encryption, firewalls, virus protection and regular data back-up.

## 05: Privacy

---

### 5.1.4 How personal information is disposed of

PALS will retain personal information for as long as it is needed for the purpose for which it was obtained and in order to comply with legal, regulatory, financial and administrative requirements.

When a person's personal information is no longer needed for the purpose for which it was obtained, PALS will take reasonable steps to destroy or permanently de-identify it. This includes secure shredding and disposal of hard copy information and permanently deleting electronic information.

## 5.2 How PALS uses and discloses personal information

PALS will use the personal information collected to help provide services or support to a person where explicit consent has been obtained, for example, through the completion of the Consent to Share Information Form or implicitly consented through an enquiry received by phone or email.

Consent must be current and reviewed at least every two years. If consent to share information has not been received within the previous two years, explicit consent must be obtained and updated before any information can be disclosed.

### 5.2.1 Disclosure of personal information

Except for the examples listed below, personal information is disclosed with third parties, such as government agencies and other service providers, with the consent of the person (or their legal representative) and where necessary for the effective provision of service and/or as required by regulation, contract or legislation. Consent may be gained on engagement with a service and/or through the completion of a Consent to Share Information Form.

PALS will always try to obtain consent before disclosing information to a third party but are permitted to share information with government agencies and non-government organisations without a person's consent if:

- there are concerns about the safety, welfare and wellbeing of children and young people, for example, as mandatory reporters, PALS are required by law to report to Child Protection in NSW and Victoria if it is suspected, on reasonable grounds, that a child or young person is at risk of significant harm;
- a request for information under Chapter 16A Request or Section 248 of the Children and Young Persons (Care and Protection) Act 1998 for statutory interventions;
- a person is a PALS Worker and there have been allegations against that person of sexual offence or misconduct to, or in the presence of, a child or any other form of harm or neglect of a child; or
- it is essential to lessen or prevent a serious threat to the life, health or safety of any person, or to public health or safety, or to take appropriate action about suspected unlawful activity or serious misconduct.

As a requirement of the funding of our services, PALS may be required to share de-identified information (where personal identifiers such as name and address have been removed) about people receiving services with the government agency accountable for the service.

## 05: Privacy

---

In accordance with contractual, regulatory and legislative requirements, PALS are obligated to report serious incidents and complaints, which may contain personal information.

### 5.3 Data Breaches

The Notifiable Data Breach Scheme requires organisations to notify particular individuals and the Office of the Australian Information Commissioner (OAIC) if an 'eligible data breach' occurs. A data breach is eligible if it's likely to result in serious harm (psychological, emotional, physical, reputational or other forms of harm) to any of the individuals to whom the information relates.

PALS recognise data breaches may fall into two (2) primary categories, serious (eligible) and minor. To ensure that breaches are responded to in an appropriate timely manner the Data Breach Response procedure must be followed. Minor breaches are those that are rectified quickly and individuals are not at risk of suffering serious harm. Eligible data breaches will result in immediate notification to individuals affected and to the OAIC.

### 5.4 Accessing and correcting personal information

Individuals have a right under the Privacy Act to access personal information PALS hold about them. Individuals may also request corrections of any personal information that is held about them, where they believe the information is inaccurate, out-of-date, incomplete, irrelevant or misleading.

To request access or seek correction of personal information, individuals may contact PALS by phone, email or in person and provide identification to prove their identity to facilitate the request. PALS will respond to requests within a reasonable period of time (usually 30 days).

The APPs outline circumstances in which PALS may refuse to give a person access or decline to correct personal information. If an access request to personal information is denied, reasonable steps are taken to give the person access to the information in an alternative form. A person will be provided with a written notice setting out the reasons for refusal, and how they can lodge a complaint about the decision.

### 5.5 Complaints

If a person believes that there has been a breach in their privacy, they can contact PALS directly or via the PALS website. Details on how to make a complaint are set out in the Complaints Management Policy, available on the PALS website.

PALS are committed to a prompt and fair resolution of complaints and will ensure that a person's complaint is taken seriously and investigated. In all cases, the person will be informed of the progress and outcome of the complaint.

If a person is not satisfied with the way a complaint has been handled, they may contact the OAIC. The Information Commissioner may not investigate if a person's complaint unless it has first been brought to the attention of PALS.

## 05: Privacy

---

Contact details for the Office of the Australian Information Commissioner:

**Telephone** 1300 363 992

**Email** enquiries@oaic.gov.au

**Post** GPO Box 5218, Sydney NSW 2001

### 5.6 Our website and social media channels

PALS uses social media platforms including Facebook, LinkedIn, Instagram, Twitter, YouTube, and Google to tailor the information delivered on social media and the PALS website to the preferences of PALS's audience.

#### 5.6.1 Website Cookies

PALS collects information from users of this website through the use of 'cookies'. Cookies allow PALS to track non-personal information about a person, such as their IP address, date and time of visit, the pages viewed, information downloaded, what browser a person is using, what search terms are used to find the PALS website and any information a person's browser may send PALS. This information will only be used for the purpose of site analysis to improve online services and a person cannot be identified from this information.

## 6. Responsibilities

### 6.1 Board

Board members are responsible to:

- Role model appropriate standards of behaviour in handling personal, sensitive and confidential information in accordance with this policy.
- Ensure that staff are educated and aware of their obligations under this policy and the law.

### 6.2 CEO

The CEO is responsible to:

- Take action to ensure that all staff and volunteers are appropriately aware of their rights and obligations under this policy.
- Take action to implement this policy, to monitor changes in Privacy Legislation, and to advise the Board on the need to review or revise this policy as and when the need arises.
- Ensure that PALS has a designated Privacy Officer, and that the Privacy Officer is appropriately trained and resourced to undertake the role.
- Ensure that breaches of this policy are investigated and resolved promptly, fairly and appropriately.
- Staff and volunteers.

### 6.3 All staff and volunteers are responsible to:

- Handle all personal, sensitive and confidential information in accordance with this policy.
- Report any known or possible breaches of this policy to Senior Management.

05: Privacy

---

**7. Supporting Documents**

- PALS Code of Conduct
- Employment Agreements
- Staff Handbook
- Privacy and Confidentiality Agreement
- Media Consent Form
- Consent to Share Information

**8. References**

- Australian Privacy Principles
- Information Privacy Principles (Vic)
- Privacy Act 1988 (Cth) Privacy and Data Protection Act 2014 (Vic)
- Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth)
- Health Records and Information Privacy Act 2002 (NSW), including the Health Privacy Principles
- Health Records Act 2001 (Vic), including the Health Privacy Principles
- National Disability Insurance Scheme Act 2013 (Cth)

---

Policy Name & Number:	05 Privacy		
Policy Type:	Governance	Personnel Responsible	CEO
Approved By:	Board	Approved Date:	October 2024
		Review Date:	July 2026
Changes:	Reference updates		