Document reference:	POLBS0011 - Information Privacy
Approved by:	QCM
Date developed:	July 2023
Review date:	July 2026

Contents of this policy

Policy Statement

James Milson Village (the Organisation) ensures that Stakeholder's personal information is collected, used, disclosed and stored according to the relevant legislation, that is – the Privacy Act 1988, the Privacy Amendment (Enhancing Privacy Protection) Act 2012, the Privacy Amendment (Notifiable Data Breaches) Act 2017 and associated Privacy Regulations and Principles.

Legislation

The Privacy Act 1988 (Privacy Act (1988) www.legislation.gov.au) , Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Privacy Amendment (Enhancing Privacy Protection) Act (2012) www.legislation.gov.au) and the Privacy Amendment (Notifiable Data Breaches) Act 2017 (Privacy Amendment (Notifiable Data Breaches) Act 2017 www.legislation.gov.au) regulate how the organisation is able to collect, use, disclose and store personal information, and how individuals may access and correct personal information held about them.
The Privacy Act defines personal information as "Information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified individual, or an individual who is reasonably identifiable".
The Australian Privacy Principles (APPs) (Australian Privacy Principles (2014), www.oaic.gov.au "Privacy Fact Sheet 17 – Australian Privacy Principles") are the cornerstone of the privacy protection framework in the Privacy Act 1988 (Privacy Act). They apply to any organisation or agency the Privacy Act covers.

There are 13 Australian Privacy Principles and they govern standards, rights and obligations around:

- the collection, use and disclosure of personal information
- an organisation or agency's governance and accountability
- integrity and correction of personal information
- the rights of individuals to access their personal information

The Australian Privacy Principles (2014) are:

1. Open and transparent management of personal information –to ensure that we manage personal information in an open and transparent way.
2. Anonymity and pseudonymity – individuals have the right not to be identified when dealing with a certain matter.
3. Collection of personal information – information collected must be reasonably necessary for the functioning of the organisation.
4. Dealing with unsolicited personal information –
5. Notification of the collection of personal information – when collecting information about an individual, the organisation must ensure that they notify that individual that this information is being collected, and for what purpose it will be used.

6. Use or disclosure of personal information – information, must not be disclosed to other organisations unless the individual has consented to this.
7. Direct marketing – information gained must not be used for direct marketing
8. Cross Border disclosure – before the organisation discloses information to an overseas entity about an individual, the organisation must ensure that it does not breach the Australian Privacy Principles.
9. Government identifiers – the organisation must not adopt a government related identifier as its own identifier or the individual
10. Quality of personal information – the organisation must ensure that information collected is accurate, up to date and complete.
11. Security of personal information – the organisation must take reasonable steps to protect the security of all personal information held.
12. Access to personal information – the organisation must upon request by the individual give the individual access to the information
13. Correction of personal information – if information held by an organisation about an individual is found to be inaccurate, out of date, irrelevant or misleading then the organisation must take all reasonable steps to correct that information.

Kinds of personal information collected.

Residents: Financial information, legal power of attorney documentation, Medicare, DVA and Centrelink entitlement numbers, date of birth, assessments and care plans and medical information other information which form a Residents medical record.
Representatives: legal power of attorney documentation, home and mobile contact details, address, email address.
Staff: home and mobile contact details, address, email address, federal police check information and statutory declaration, payroll information – superannuation and bank details, next of kin details, education and qualification records, records of any disciplinary action taken, correspondence, sick leave records.
Volunteers: home and mobile contact details, address, email address, federal police check information and statutory declaration, next of kin details, education records, correspondence, privacy and confidentiality agreement.
Contractors: Contact details, bank details, federal police check information, contracts.
Committee: home and mobile contact details, address, email address, federal police check information and statutory declarations, key personnel documentation.

How information is collected and held

- Information is collected upon admission to/commencement with the organisation in both electronic and paper-based format.

- Information is stored both electronically and in paper-based format.
- Resident care information is stored on the computerised care planning system and in paper-based files stored in the Care staff offices.
- Resident financial information is stored on the financial accounting program and in paper-based files stored in administration offices.
- Staff information is held in their paper-based personnel file located in the administration offices which are locked after hours. Payroll information is stored on the financial accounting program and in paper-based files stored in the administration offices. Only Administration staff have access to this information.
- Information pertaining to the Police checks of staff, volunteers and contractors is collected through an online police check system and stored through their database which is password protected. Only the Administration staff have access to this system. This information is also stored on the financial system. Only Administration staff have access to this system.
- Volunteer information is stored in a locked filing cabinet in Administration areas.
- Contractor information is stored on the financial accounting program. Computerized systems and in paper-based files stored in the administration office which is locked after hours.
- Committee of Management information is stored on the financial accounting program and in paper-based files stored in the administration office which is locked after hours.
- All computers within the Organisation are password protected. Each staff member is able to access only the information relevant to the performance of their role. Under no circumstance is a staff member to divulge their password to another person.
- Passwords for the server are known only by the senior executive and Information Technology contractor.
- Only the senior executive has administration rights to the Financial Software program and the computerised care planning system. Privacy and confidentiality of information is embedded within the contracts of external service providers.
- Staff and volunteers sign Confidentiality Agreement on commencement to ensure they comply with their legislative responsibilities in relation to privacy and confidentiality.

Notification

On admission, Residents and Representatives are provided with Privacy Disclosure Statement which they are required to sign. This document outlines the circumstances under which personal information is collected, used, disclosed and stored.

Purposes for which information is collected, held, used and disclosed

Residents: Health Information is collected and held to record, monitor and assess the effectiveness and appropriateness of care and to determine if changes are required to care practices. Financial information

is held to ensure that appropriate fees and charges and accommodation payments are charged. Information pertaining to Care Recipients' nominated Power of Attorney/Guardian or Next of Kin is collected and held to ensure that personal Care Recipient information is shared with only the authorised individual.

Staff, Volunteers, Contractors and Board: Financial information (Bank Accounts, Superannuation) is collected and held to ensure adequate payment for services is received. Evidence of Police checks and statutory declarations are held to ensure to safety and protection of all Care Recipients residing within the organisation. Information about the performance of a staff member, volunteer, contractor or Committee member may be collected and held for the purposes of performance management, however in relation to staff information, can only be held for the period as specified in their respective Award and/or Enterprise Bargaining Agreement. Refer further to Human Resources

Information can only be disclosed with the expressed or written consent of the individual to whom it relates with the following exceptions:

- If the use/disclosure is requested or authorised under an Australian law or a court/tribunal order
- A health situation occurs necessitating use/disclosure
- The Organisation reasonably believes that use/disclosure of the information is necessary for use by an enforcement agency

Accessing personal information

If an individual's personal information is held by the Organisation, then the Organisation must, on written request by the individual, provide access to this information. The request must be made using **Request to access Information form**.

The Organisation have a responsibility under the Aged Care Act 1997 and other laws to give people access to their own health records. In aged care legislation, providing access to care records is a requirement of the Charter of Care Recipients' Rights and Responsibilities.

If a representative is seeking care records of someone they do not legally represent, there are restrictions in the Australian Privacy Principles and the Aged Care Act 1997 about disclosing information. The representative must have consent from the person receiving care or their legal representative authorising access to their care records.

A request for information can be declined under the following circumstances :

- If the Organisation believes that giving access would pose a serious threat to the life, health or safety of an individual
- Giving access would have unreasonable impact on the privacy of other individuals
- The request is seen to be vexatious or frivolous
- The information relates to existing or anticipated legal proceedings between the Organisation and the Individual and would not be accessible by the process of discovery in those proceedings
- Lack of authorised evidence (e.g., power of attorney / executor of estate / court order) to act on behalf of the person receiving care

- Giving access would reveal the intention of the Organisation in relation to negotiations with the individual in such a way as to prejudice those negotiations
- Giving access would be unlawful
- Denying access is required or authorised by or under an Australian law or court/tribunal order
- The Organisation has reason to suspect an unlawful activity or misconduct of a serious nature AND giving access would be likely to prejudice the taking of appropriate action in that matter
- Giving access would be likely to prejudice enforcement related activities conducted by an enforcement body.
- Giving access would compromise a commercially sensitive process.

The Organisation will respond within 14 days once a request has been received. In the response there will be an estimate of any charges that may apply to the request.
The Organisation will notify of its decision within 30 days unless that time has been extended. If a document contains information about a third party, the Organisation may need to consult with them and may need to extend the time to give a decision by another 30 days. The Organisation may also seek agreement to extend the time by up to 30 days if the request is complex.
The Organisation must give access to the information in the manner requested by the individual within a reasonable period after the request is made. If access is refused, the Organisation must state the reasons and the mechanisms for complaint.

Requesting correction to personal information

The Organisation must take reasonable steps to ensure that personal information held is current, accurate and complete.
Should an individual believe that information held about them is incorrect, they can request this be amended or corrected.
The Organisation must respond to the request within a reasonable timeframe. and must not charge individuals for making this correction.
Should the Organisation refuse to amend or correct personal information about an individual, they must provide written reasons for the refusal, as well as relevant complaint mechanisms (refer below to Complaining about a Privacy Breach)

Complaining about a Privacy Breach

The Chief Executive Officer (CEO) has been nominated as the Privacy Officer for JMV (“the Organisation”). In the first instance, any complaints made in relation to how the Organisation manages individuals’ personal information should be made to the General Manager. This can be verbal or written using Feedback Form.

Should the complainant not be satisfied with the outcome of their complaint, or if they have not received a response within 30 days, they can complain to the Office of the Australian Information Commissioner (OAIC) using the online Complaints Form . This is located at www.oaic.gov.au
The OAIC has the power to investigate complaints made about privacy if it is clear there has been a breach in the Privacy Act 1988 and associated amendments and principles. The OAIC acts as an impartial regulator.
Where a notifiable data breach has occurred, which is likely to result in serious harm there are now clear guidelines in relation to the reporting of that breach (refer below).

Notifiable Data Breaches

As a Health Service Provider, and under the Privacy Amendment (Notifiable Data Breaches) Act 2017 the Organisation is obliged to report when a data breach has occurred, which is likely to result in serious harm to any individuals whose personal information is involved in the breach.
If there are reasonable grounds to believe there has been an eligible data breach then there is an obligation to notify the Office of the Australian Information Commissioner (OAIC) and the individuals whose data was affected or individuals who are at risk with:

- The identity and contact details of the organisation
- a description of what occurred/the data breach
- the kinds of information concerned; and
- the recommended next steps that individuals affected should take in response to the data breach.

For notifiable breaches, and further resources about notifiable data breaches, an online notification form can be found at the OAIC website on www.oaic.gov.au or for more information, phone contact can be made with the OAIC on 1300 363 992.
Alternately, the organisation may wish to prepare a statement using a Word Document and provide it to the Commissioner by sending it to:

Email: enquiries@oaic.gov.au
Fax: +61 2 9284 9666
Post: GPO Box 5218 Sydney NSW 2001

An 'eligible data breach' arises when the following criteria are satisfied –

1. There is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information and;
2. This is likely to result in serious harm to one or more individuals and;
3. The organisation been unable to prevent the likely risk of harm with remedial action

To determine whether an individual is at risk of serious harm consideration must be given to factors such as the sensitivity of the information, whether the information is protected by one or more security measures, the kind of persons who could obtain the information and the nature of the harm.

The nature of harm

In assessing the risk of serious harm, the organisation should consider the broad range of potential kinds of harm that may follow a data breach.
It may be helpful when considering the likelihood of harm to consider several scenarios that may result in serious harm and the likelihood of each.
Examples may include –

- Identify theft
- Significant financial loss
- Threats to an individual's physical safety
- Loss of business or employment opportunities
- Humiliation, damage to reputation or relationships
- Workplace or social bullying or marginalisation

Disclosure of information to overseas recipients

Where an overseas entity has requested personal information about a Resident or staff member, the Organisation must take care to ensure that, in providing this information, the overseas entity does not breach the Australian Privacy Principles .
Where an overseas entity has requested personal information about a Resident or staff member, the individual to whom the information is related (or their nominated representative) must provide written consent for this information to be disclosed.