# Privacy and Dignity

**Privacy Policy**

## Scope of Policy and Source of Obligation

A key aspect of dignity and respect is making sure a resident / client's privacy is respected. In the course of Westmont Aged Care Services activities we respect, manage and protect personal information in accordance with the Aged Care Quality Standards, the Privacy Act 1988 (Cth) (Privacy Act) and the 13 Australian Privacy Principles (APPs).

## Scope of Policy

This policy outlines the circumstances in which we obtain personal information, how we use and disclose that information, and how we manage requests to access and/or change that information.

## What is Personal Information and How Do We Collect It?

Personal information is information or an opinion about an individual from which they can be reasonably identified. Depending on the circumstances, we may collect personal information from the individual in their capacity as a resident / client, contractor, volunteer, stakeholder, job applicant, visitors or others that come into contact with the organisation.

In the course of providing aged care services we may collect and hold:

- Personal Information including names, addresses and other contact details, dates of birth, next of kin details, photographic images and financial information.
- Sensitive Information (particularly in relation to resident / client records) including government identifiers (such as TFN), religious beliefs, nationality, country of birth, professional memberships, powers of attorney, guardianship orders and criminal records.
- Health Information (particularly in relation to resident / client records) including medical records, disabilities, and psychological reports.

As part of our recruitment processes for employees, contractors and volunteers, we may collect and hold:

- Personal Information including names, addresses and other contact details, dates of birth, financial information, citizenship, employment references, regulatory accreditation and driver's licence information.
- Sensitive Information including government identifiers (such as TFN), nationality, country of birth, professional memberships and criminal records.
- Health Information (particularly in relation to prospective workers and resident / client records) including medical records, disabilities, psychological reports, vaccination evidence.

Generally, we will seek consent from the individual in writing before we collect their sensitive information (including health information).

Employee records are not covered by the APPs where they relate to current or former employment relations between the organisation and the employee.

However, a current or former employee's health records are covered by the Victorian Health Privacy Principles.

## Collection of Personal Information

The collection of personal information depends on the circumstances in which Westmont is collecting it. If it is reasonable and practical to do so, we collect personal information directly from the individual.

## Solicited Information

Westmont has, where possible, attempted to standardise the collection of personal information by using specifically designed forms (e.g. a Health Information Disclosure Form). However, given the nature of our operations we also receive personal information by email, letters, notes, via our website, over the telephone, in face-to-face meetings, through financial transactions and through surveillance activities such as the use of CCTV security cameras or email monitoring.

We may also collect personal information from other people (e.g. a third-party administrator, referees for prospective employees) or independent sources. However, we will only do so where it is not reasonable and practical to collect the personal information from the individual directly.

## Unsolicited Information

Westmont may be provided with personal information without seeking it through our normal means of collection. This is known as “unsolicited information” and is often collected by:

- misdirected postal mail – letters, notes, documents
- misdirected electronic mail – emails, electronic messages
- employment applications sent to us that are not in response to an advertised vacancy
- additional information provided to us which was not requested.

Unsolicited information obtained by Westmont will only be held, used and or disclosed if it is considered as personal information that could have been collected by normal means. If that unsolicited information could not have been collected by normal means then we will destroy, permanently delete or de-identify the personal information as appropriate.

## Collection and Use of Sensitive Information

We only collect sensitive information if it is:

- reasonably necessary for one or more of these functions or activities, and we have the individual’s consent
- necessary to lessen or prevent a serious threat to life, health or safety
- another permitted general situation
- another permitted health situation.

We may share sensitive information with other entities in our organisation structure, but only if it is necessary for us to provide our products or services.

## How Do We Use Personal Information?

Westmont only uses personal information that is reasonably necessary for one or more of our functions or activities (the primary purpose), a related secondary purpose that would be reasonably expected by you, or for an activity or purpose to which you have consented.

Our primary uses of personal information include, but are not limited to:

- providing aged care services
- satisfying our legal obligations including our duty of care obligations

- keeping resident / clients, their carers/representatives and communities informed about relevant matters through correspondence, newsletters and magazines
- marketing, promotional and fundraising activities
- supporting the activities of the Board of Directors
- supporting community-based causes and activities, charities and other causes in connection with the organisation's functions or activities
- helping us to improve our day-to-day operations including training our workers
- systems development, developing new programs and services, undertaking planning, research and statistical analysis
- administration, including for insurance purposes
- the employment of staff
- the engagement of contractors and volunteers.

We will only use or disclose sensitive or health information for a secondary purpose if you would reasonably expect us to use or disclose the information, and the secondary purpose is directly related to the primary purpose.

We may disclose personal information to related bodies corporate, but only if necessary, for us to provide our services.

We will not disclose information about an individual to overseas recipients (for example, to facilitate overseas travel) unless it is necessary and with their consent.

## Storage and Security of Personal Information

Westmont stores Personal Information in a variety of formats including, but not limited to:

- databases
- hard copy files
- personal devices, including laptop computers
- third party storage providers such as cloud storage facilities
- paper based files.

Westmont takes all reasonable steps to protect the personal information we hold from misuse, loss, unauthorised access, modification or disclosure.

These steps include, but are not limited to:

- restricting access and user privilege of information by type of worker, depending on their role and responsibilities
- ensuring workers do not share personal passwords
- ensuring hard copy files are stored in lockable filing cabinets in lockable rooms, and workers' access is subject to user privilege
- ensuring access to Westmont Aged Care Services premises are secured at all times
- implementing physical security measures around the buildings and grounds to prevent break-ins
- ensuring our IT and cyber security systems, policies and procedures, are implemented and up to date
- ensuring workers comply with internal policies and procedures when handling the information
- undertaking due diligence with respect to third party service providers who may have access to personal information, including customer identification providers and cloud service providers, to ensure as far as practicable that they are compliant with the APPs or a similar privacy regime
- the destruction, deletion or de-identification of personal information we hold that is no longer needed or required to be retained by any other laws.

Our public website may contain links to other third-party websites outside of Westmont. Westmont is not responsible for the information stored, accessed, used or disclosed on such websites and we cannot comment on their privacy policies.

## Responding to Data Breaches

Westmont will take appropriate, prompt action if we have reasonable grounds to believe that a data breach has, or is suspected to have, occurred. Depending on the type of data breach, this may include a review of our internal security procedures, taking remedial internal action, and notifying affected individuals and the Office of the Australian Information Commissioner (OAIC).

If we are unable to notify individuals, we will publish a statement on our website and take reasonable steps to publicise the contents of this statement.

## Disclosure of Personal Information

Personal information is used for the purposes for which it was given to Westmont, or for purposes which are directly related to one or more of our functions or activities.

Personal information may be disclosed to government agencies, other resident / clients, other aged care providers, recipients of our publications, visitors, carers, advocates, our services providers, agents, contractors, business partners, related entities and other recipients from time to time, if the individual:

- has given consent; or
- would reasonably expect the personal information to be disclosed in that manner.

Westmont may disclose personal information without consent or in a manner which an individual would reasonably expect if:

- we are required to do so by law
- the disclosure will lessen or prevent a serious threat to the life, health or safety of an individual, or to public safety
- another permitted general situation applies
- disclosure is reasonably necessary for a law enforcement related activity
- another permitted health situation exists.

Refer to our Privacy Program for more information on permitted general situations and permitted health situations.

## Disclosure of Personal Information to Overseas Recipients

Personal information about an individual may be disclosed to an overseas organisation in the course of providing our services. For example, when storing information with a “cloud service provider” which stores data outside of Australia.

We will, however, take all reasonable steps not to disclose an individual’s personal information to overseas recipients unless:

- we have the individual’s express or implied consent;
- we have satisfied ourselves that the overseas recipient is compliant with the APPs, or a similar privacy regime;
- we form the opinion that the disclosure will lessen or prevent a serious threat to the life, health or safety of an individual or to public safety; or
- we are taking appropriate action in relation to suspected unlawful activity or serious misconduct.

## Mental Capacity, Privacy and Consent

Where a resident / client lacks the capacity to consent to the use of their personal information, we will seek consent from their representative or guardian in accordance with Commonwealth, state and territory guardianship laws.

## The Quality of Personal Information

We take all reasonable steps to ensure the personal information we hold, use and disclose is accurate, complete and up to date, including at the time of using or disclosing the information.

If Westmont becomes aware that the Personal Information is incorrect or out of date, we will take reasonable steps to rectify the incorrect or out of date information.

## Access and Correction of Personal Information

You may submit a request to us to access your personal information we hold, or request that we change your personal information. Upon receiving such a request, we will take steps to verify your identity before granting access or correcting the information.

If we reject the request, you will be notified accordingly. Where appropriate, we will provide the reason/s for our decision. If the rejection relates to a request to change personal information, an individual may make a statement about the requested change and we will attach this to their record.

## Complaints

You can make a complaint about how Westmont manages personal information, including a breach of the APPs, by notifying us in writing as soon as possible. We will respond to the complaint within a reasonable time (usually no longer than 30 days) and we may seek further information in order to provide a full and complete response.

Westmont does not charge a fee for the handling of complaints.

If you are not satisfied with our response, you may refer the complaint to the OAIC. A complaint can be made using the OAIC online https://www.oaic.gov.au/privacy/privacy-complaints or by mail, fax or email.

A referral to OAIC should be a last resort once all other avenues of resolution have been exhausted.

## How to Contact Us

Westmont can be contacted about this Privacy Policy or about personal information generally, by:

- emailing awilliamson@westmont.org.au
- calling 02 6043 9843
- writing to Westmont and addressing the letter to the People and Culture Manager.

If practical, you can contact us anonymously (i.e. without identifying yourself) or by using a pseudonym. However, if you choose not to identify yourself, we may not be able to give you the information or provide the assistance you might otherwise receive if it is not practical to do so.

## Changes to Our Privacy and Information Handling Practices

This Privacy Policy is subject to change at any time. Please check our Privacy Policy on our public website regularly for any changes.

## Related Documents and Forms

Insert List and Link to Additional Privacy Related Documents (e.g. Personal Information Audit)

This Privacy Policy was last reviewed: December 2020