PRIVACY POLICY

Name of Policy:	Privacy Policy
Approval Authority:	Victorian State Council / SVDPV-VCV Board
Date effective:	19 December 2025
Due to be reviewed:	19 December 2028
Accountable Officer:	Chief Executive Officer
Responsible Officer:	General Counsel
Policy applies to:	Victorian State Council and its corporate entities - • St Vincent de Paul Society Victoria • VincentCare Victoria • VincentCare Community Housing

1. Purpose

1.1 The purpose of this Policy is to outline how the Society protects the privacy of individuals whose Personally Identifiable Information (PII) it collects, holds and uses.

2. Scope

2.1 This Policy applies to everyone who is part of the St Vincent de Paul Society Victoria and its corporate entities St Vincent de Paul Society Victoria, VincentCare Victoria and VincentCare Community Housing (collectively 'the Society'). This includes our members, directors, employees, volunteers, and contractors (collectively 'Our People').

2.2 This Policy applies to all of Our People when conducting any Society work or activity.

2.3 The Policy covers information and records relating to all individuals with whom the Society interacts across its operations and entities, including:

a) companions, clients, residents and renters;

b) donors, supporters, sponsors and bequestors;

c) retail customers; and

d) individuals who access, use and interact with our website.

2.4 This Policy does not apply to employee or employment records or information. The handling of employee information by a private sector employer is exempt from the Privacy Act if it is directly related to the current or former employment relationship.

Nonetheless, the Society will exercise diligence in keeping employees' personal information secure and appropriately managed in alignment with the general privacy principles expressed in this policy.

3. Policy

CORE PRINCIPLES

3.1 The Society is committed to fulfilling its legal responsibilities with regard to the collection, use, management and sharing of personal information, and to informing clients, staff and relevant others about their privacy rights.

3.2 The Society complies with the requirements of the Australian Privacy Principles (APPs) and Health Privacy Principles in the handling of all PII.

3.3 Clear, accessible information is available to all people who interact with the Society relating to:

a) how we collect PII;

b) how we obtain and record consent to the collection and uses of PII;

c) how we use PII;

d) how we record and store PII;

e) how, to whom, and in what circumstances we will disclose PII, including the times when we can or must disclose PII without consent of the person concerned;

f) the rights and responsibilities of people whose information we hold to access and correct information;

g) the length of time we will maintain PII in our custody; and

h) the steps we will take to ensure that information that is no longer required is securely destroyed in accordance with our *Retention and Disposal Schedule*.

3.4 The Society will take reasonable steps to protect the PII that it collects and stores from misuse, interference and loss, and from unauthorised access, modification or disclosure.

OPEN AND TRANSPARENT MANAGEMENT OF INFORMATION AND CONSENT

3.5 Individuals interacting with the Society will be informed of their rights and responsibilities in relation to privacy, and the extent and limitations of consent (where safe, reasonable and appropriate) under relevant legislation.

3.6 Where individuals wish to remain anonymous or pseudonymous, they may do so, but it will be explained that this may limit, or in some cases prevent, service provision.

3.7 For privacy consent to remain valid, the Society will ensure that:

a) review of consent with client/resident takes place regularly while the person is engaged with the Society;

b) the individual is adequately informed before giving consent;

c) the individual gives consent voluntarily;

d) the consent is current and specific; and

e) the individual has the capacity to understand and communicate.

COLLECTION OF PII

3.8 The Society will only collect PII for purposes that are directly related to our functions or activities. As the collector of information, the Society must justify why information is being collected and how it will be used.

3.9 The primary purposes for which the Society collects PII are to:

a) provide, administer, improve and personalise our services and goods;

b) engage with customers, supporters, testators and donors;

c) process and manage donations, bequests and payments;

d) identify and verify the identity of individuals;

e) assess applications for support or assistance;

f) assess membership, employment and volunteering applications;

g) meet our contractual, funding and regulatory obligations;

h) conduct surveys and research; and

i) respond to queries or concerns.

3.10 The Society also collects information about individuals who access, use and interact with our online services using a range of technical tools including cookies and Google Analytics. Website users may decline to allow the use of these tools via their browser settings.

3.11 In most instances, the Society will collect information directly from the individual.

3.12 We may also collect information from a third party or a publicly available source, but only if the individual has consented to such collection or would reasonably expect the Society to collect information in this way.

3.13 We will take reasonable steps to notify the individual that the collection has occurred and seek their consent to store this information.

3.14 We will only collect Sensitive Information directly from an individual or their nominated representative.

USE AND DISCLOSURE OF PII

3.15 The Society will only disclose PII for a required and lawful purpose, and will disclose the minimum amount of information required to achieve the purpose.

3.16 The Society may use and disclose personal information to:

a) provide, administer, improve and personalise services and goods;

b) provide support and assistance to those in need;

c) identify and support people who may need to be referred to external services;

d) engage in direct marketing to past and potential donors and supporters;

e) fulfill obligations under the Victorian Government's Family Violence Multi Agency Risk Assessment and Management Framework (MARAM) schemes (see *Privacy – Information Sharing Schemes Procedure* for details);

f) authenticate and verify individual identity for system access purposes;

g) comply with lawful information requests from police, courts, government agencies and lawyers in connection with suspected fraud, misconduct or unlawful activity; and

h) comply with our funding and contractual obligations.

3.17 While the Society may use PII to provide promotional materials and marketing communications, all people can choose to opt out of these communications and this will be respected.

SECURITY OF PII

3.18 The Society stores and manages PII in accordance with the Australian Privacy Principles. All reasonable steps are taken to ensure the Society has safe systems, processes, and training in place to protect PII.

3.19 The Society ensures that all PII is maintained in a manner or format that allows for it to be accessible and readable for the entire required lifespan of the PII, as identified in the Society's RDS.

3.20 The Society's sensitivity data labelling scheme is used to identify and manage PII in an appropriate way.

3.21 When using open access (unsecured) Artificial Intelligence tools, the Society will ensure no PII is included in data sets or otherwise put at risk of inadvertent disclosure.

3.22 If a data breach of PII occurs, the *Data Breach Response Plan* provides direction on how the Society will respond, including identifying, assessing, reporting and remediating data breaches.

DISPOSAL OF PII (INCLUDING UNSOLICITED PII)

3.23 Where individuals send unsolicited PII to the Society, it will be retained and treated as solicited PII if:

a) the unsolicited PII is information contained in a public record;

b) the unsolicited PII is information that the Society would have been entitled to collect and has a purpose for; or

c) the unsolicited PII is so entwined with the solicited PII as to make it impossible to meaningfully disentangle the two.

3.24 If unsolicited PII does not meet one of the three criteria above, it will be destroyed as soon as is reasonably possible.

3.25 All solicited PII will be retained for the required period identified in the Society's *Retention and Disposal Schedule*, which considers all legislative requirements and business needs.

3.26 When PII is due to be disposed of in accordance with the RDS, an organisational check should take place to ensure that the disposal is appropriate in the circumstances. If disposal is authorised, the method of destruction chosen will be:

a) secure;

b) complete; and

c) recorded.

ACCESS TO PII AND RIGHT TO CORRECTIONS

3.27 Individuals are entitled to confirm that their PII is being stored by the Society, and are entitled to access this information.

3.28 Information requested must be provided to the individual as soon as possible and within 30 days of the request, unless:

a) the Society reasonably believes that giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety; or

b) giving access would have an unreasonable impact on the privacy of other individuals; or

c) giving access would be unlawful; or

d) denying access is required or authorised by or under an Australian law or a court/tribunal order; or

e) the Society has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the Society's functions or activities has been, is being or may be engaged in and giving access would be likely to prejudice the taking of appropriate action in relation to the matter; or

f) giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body.

3.29 PII can be corrected if it is inaccurate, out-of-date, incomplete, irrelevant or misleading. Factual corrections must be made. Differences of opinion/s can be noted.

3.30 If the Society identifies information that meets one or more of the above criteria, it has an obligation to take reasonable steps to correct it.

3.31 Where an individual believes the PII the Society holds about them meets one or more of the above criteria, they can request that it be corrected. Corrections made by the individual can add to the record, but never deleted from the record.

4. Definitions

4.1 Table One – Definitions

WORD/ TERM	DEFINITION
Personally Identifiable Information (PII)	**Personal Information** (referred to in this policy as "**PII**") is any information or an opinion about an identified individual or an individual who can be reasonably identified from the information or opinion. It may include a person's name, address, telephone number, email address, date of birth, signature, salary and banking details. It includes **Health Information** and **Sensitive Information**.
Data breach	A data breach occurs when PII is lost or subjected to unauthorised access, modification, use or disclosure, or other misuse. Data breaches are not limited to malicious actions, such as theft or 'hacking', but may arise from internal errors or failure to follow information handling policies that cause accidental loss or disclosure.
Health Information	Any **Personal Information** or opinion about an individual's: ▪ physical, mental or psychological health ▪ disability ▪ health services provided or to be provided in future Health Information also includes any Personal Information collected in the course of providing health services.
Sensitive Information	**Personal Information** that includes information or opinion about an individual's health, genetics, race, political opinion, religion, philosophical beliefs, trade union membership, sexual preference and criminal record.

WORD/ TERM	DEFINITION
Unsolicited PII	PII is unsolicited if the organisation took no active steps to collect it. Examples of unsolicited personal information include: ▪ misdirected mail ▪ correspondence from members of the community ▪ a petition that contains names and addresses ▪ an employment application sent on an individual's own initiative and not in response to an advertised vacancy Unsolicited PII also includes information provided in excess of that requested or required. For example if an individual completes an application form but chooses to attach financial records.

5. Supporting Documentation

Privacy Procedure
Privacy - Information Sharing Schemes Procedure
Privacy – Good Works Client Records Procedure
Privacy - VincentCare Client Records Procedure
Privacy - VCCH Client Records Procedure
Data Breach Response Plan

Data Governance Framework
Data Management Policy
Data Labelling Schedule
Data Retention and Disposal Schedule

ICT Acceptable Use Policy
Use of Artificial Intelligence Policy

6. Legislative and Regulatory Obligations and Quality Alignment

6.1 This Policy supports the Society's alignment with the following legislation or quality standards:

Privacy Act 1988 (Cth)
Spam Act 2003 (Cth)
Privacy & Data Protection Act 2014 (Vic)
Health Records Act 2001 (Vic)
Family Violence Protection Act 2008 (Vic)