St Vincent de Paul Society NSW
good works

Privacy Management Policy

Document number: PO2023-02

Approval

Policy owner	*Executive Director, Governance, Legal and Risk*		
Approved by	*Board of Directors*		
Date approved	*Board of Directors – 01 June 2023* *State Council – 17 June 2023*	*Review date*	*17 June 2026*

Purpose

1. The purpose of this Privacy Management Policy (**Policy**) is to establish minimum requirements to ensure that the St Vincent de Paul Society NSW (**Society**) manages Personal Information in a manner which complies with applicable legislation, regulations and the Society's other relevant policies and procedures.

2. The Society will also maintain a publicly available Privacy Policy, in accordance with the requirements of the Privacy Act, which provides general information on how the Society collects and manages Personal Information, how individuals may access and correct records containing their Personal Information, and how they may make a complaint about a breach of privacy.[1]

3. This Policy also summarises the requirements and process for reporting an Eligible Data Breach.

Scope

4. This Policy is an internal (non-public) policy, which applies to all Society Personnel (including members, volunteers and employees).

5. This Policy covers all Personal Information, which may include Sensitive Information and Health Information, that is collected:

   - regarding Society staff, contractors, applicants for employment, members and volunteers
   - regarding individuals who access or receive Society services, their carers or family members and other people that have contact with the Society
   - regarding donors and prospective donors for fundraising purposes.

6. Where a funding agreement has specific requirements pertaining to the collection and storage of Personal Information that are outside this Policy, a separate procedure or protocol may also exist or be developed.

Definitions

7. Capitalised words signify a word or term that is defined for this Policy. Relevant definitions are contained in **Appendix 1**.

Related policies and procedures

8. Related policies, procedures and other documents at the time of approval of this Policy include:

   - *Acceptable Use of Technology Policy*
   - *Code of Conduct*
   - *Data Breach Response Plan*
   - *Feedback and Complaints Policy*
   - *NSW Media Policy and Procedures*

[1] Refer https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-1-app-1-open-and-transparent-management-of-personal-information for guidance on development of a Privacy Policy

- *Procurement Policy*
- *Records Management Policy*
- *Safeguarding Children and Young People Policy*
- *Social Media Policy*
- *St Vincent de Paul Society NSW Privacy Policy (public document)*
- *St Vincent de Paul Society National Council Privacy Policy (public document)*
- *Vendor Information Security Agreement (applicable to suppliers)*

Policy principles

9. ***The Society is committed to protecting privacy of Personal Information***

   The Society recognises the importance of, and is committed to, protecting an individual's dignity, including rights to privacy of their Personal Information.

10. ***Information must be collected, used and disclosed in accordance with applicable laws***

    The Society will comply with Australian Privacy Laws (including those which protect specific types of personal information in service delivery to children, older people and people with disability). The Society will develop, communicate and implement its policies, practices, procedures and systems in compliance with Australian Privacy Laws.

11. ***The Society will communicate clearly with individuals in relation to privacy and obtain necessary consents for use of Personal Information***

    A Privacy Collection Statement will be provided at or before (or as soon as practicable following) the collection of an individual's Personal Information, to ensure that the individual understands their rights to privacy and confidentiality, what Personal Information is being collected, used, stored and disclosed, and why.

    The Society respects the privacy of children and young people, and people with disability. The Society takes reasonable steps, including using appropriate language and modes of communication, when interacting with individuals.

12. ***Direct marketing – opt-outs***

    Individuals will be offered a simple option available to opt out of receiving further information or correspondence if they no longer wish to receive communication from the Society.

13. ***Australian Government identifiers will not be used for any purpose other than those for which they were collected***

    Under Australian Privacy Laws, the Society is not permitted to use any government assigned identifier (e.g. Centrelink Customer Reference Number (CRN) or a Medicare number) as a primary form of identification, and such identifiers must be used strictly for the limited purpose for which they were collected. The Society will develop and maintain practices and procedures which comply with these restrictions.

14. ***The Society will support an individual's right of access to their information and their right to make a complaint***

    The Society acknowledges and supports an individual's right to access and correct their Personal Information, or to complain about a privacy related matter.

15. ***The Society will comply with the notifiable data breach requirements***

    The Society will ensure that appropriate notifications are made to the Office of the Australian Information Commissioner (OAIC) and affected individuals in the event of an Eligible Data Breach.

Personal Information collected by the Society

16. The Society may collect Personal Information required to carry out its functions or activities. These include service delivery, referrals, fundraising and communication, complaints handling and reporting. It also includes information that individuals provide to the Society through its websites, online presence or in person. The Society also collects Personal Information where necessary or required by law.

    Information about People-We-Assist

17. The Society collects Personal Information about People-We-Assist:

    - directly with the individual's consent; or
    - through the individual's Authorised Representative (such as a carer or family member), or a partnering service or government agency with the individual's consent.

18. The Society may sometimes be required to collect Sensitive Information from individuals to provide assistance. Such assistance could include facilitating arrangements with, or on behalf of, individuals for financial assistance, accommodation, community engagement, medical and/or mental health assistance.

19. The Society will limit the collection, storage, use and disclosure of Sensitive Information to instances where the information is:

    - directly relevant to the purpose for collection
    - reasonably necessary to carry out its functions or activities, or
    - required by law.

20. The Society must explain to individuals the purpose for which Sensitive Information will be collected and used, provide individuals the opportunity to discuss any concerns they may have, and record whether consent was given to use and disclose the Sensitive Information.

    Information about people who help the Society carry out its good works

21. The Society may also collect information regarding applicants for employment, staff members, volunteers or contractors (including information contained in job applications; professional development history; salary and payment information; superannuation details; medical information (for example details of disclosed disabilities and/or allergies, immunisation, medical certificates); emergency and/or family contact information; leave details; and workplace surveillance information.

22. The Society may engage third parties to provide limited Personal Information for marketing and fundraising purposes. If individuals who are contacted for marketing and fundraising purposes, no

longer wish to be contacted for those reasons then they must be able to easily opt out of further contact.

Information collected from visitors to the Society's premises

23. The Society may also collect Personal Information, including Sensitive Information, in relation to visitors to its offices or other business premises, only as authorised or required by law or otherwise permitted under Australian Privacy Laws.

Recording and surveillance

24. The Society will not record telephone conversations for quality, compliance and training purposes without the consent of the parties to the call.

25. The Society may use GPS tracking devices in its vehicles in accordance with relevant legislation and the ***Motor Vehicle Policy***.

26. Workplace surveillance information, including video; work emails and private emails (when using work email address); and Internet browsing history may be collected as outlined in the ***Acceptable Use of Technology Policy***.

27. The Society may also use surveillance cameras in retail and other premises, subject to complying with the requirements of relevant legislation, including the requirement for appropriate signage on site and provision of notice to employees and residents.

Purposes for collection, holding and use of Personal Information

28. The Society will collect, hold and use Personal Information:

- to advise about, assess eligibility for and provide services to People-We-Assist;
- to meet funding, professional and legal obligations in relation to the provision of services;
- to effectively undertake its business activities and functions, including:
    - keeping an individual's records and contact details up-to-date
    - complying with industrial relations, human resources, and workplace health and safety obligations including workplace claims management systems
    - processing and responding to complaints
    - marketing and communications
    - responding to media requests (these are referred to the Media and Communications Team who will comply with the privacy requirements in the ***NSW Media Policy and Procedure****)*
    - organisational planning
    - service development and quality control
    - research, monitoring, advocacy and evaluation
    - publishing de-identified Personal Information in submissions and reports
    - meeting audit and regulatory reporting requirements, usually through the provision of de-identified Personal Information
    - complying with any law or court/tribunal orders

- complying with regulatory authorities and government requirements, and
- fundraising purposes.

Collection of Personal Information

Collection of Personal Information from the individual

29. The Society's first and preferred approach is to collect information directly from the relevant individual wherever possible, and to ensure that they have provided informed consent.

30. Where the Society seeks Personal Information from individuals who require assistance to provide this information directly, the Society will take the necessary steps to explain the individual's right to privacy and to obtain consent in an accessible format. This may include the use of appropriate written, picture or other types of formats. The Society will record the steps taken to explain and achieve informed consent in the notes of client meetings and store these securely in personal record files.

Collection of information from third parties and other sources

31. The Society may sometimes collect Personal Information about an individual from publicly available sources, or from third parties with consent of the relevant individual.

32. Examples of publicly available sources would include magazines, books, articles in newspapers and material available on the public internet.

33. Third parties who may be authorised by an individual to release Personal Information to the Society would include: the individual's carer, guardian, advocate or other authorised representative; an individual's medical and/or health professional; government or non-government agencies that the Society partners with to deliver services; law enforcement agencies; parties to a complaint; or prescribed bodies permitted to provide information relating to the safety, welfare and wellbeing of a child or young person under Chapter 16A of the *Children and Young Persons (Care and Protection) Act 1998*. Where Personal Information about an individual is to be collected from a third party, Society Personnel must first ensure that the individual has given their consent or that the third party has the appropriate authority, before collecting the information.

34. Where the Society collects Personal Information about an individual from a third party, the Society will take reasonable steps before the time of, or at the time of collection; or as soon as practicable after collection; to let the individual or their authorised representative know the circumstances of the collection and provide them with a copy of the applicable Privacy Collection Statement.

35. In connection with the Society's fundraising purposes, an individual's Personal Information may be provided to the Society by another charity or a data co-op, to increase its donor base.

Privacy Collection Statements

36. Under Australian Privacy Laws, the Society must take reasonable steps either to notify the individual of certain matters or to ensure the individual is aware of those matters, at or before the time that the Personal Information is collected, or as soon as practicable afterwards.

37. The Society will develop and maintain Privacy Collection Statements relevant to each of the circumstances in which Personal Information is collected. For example, a Privacy Collection Statement must be included in the materials and documentation which is provided to a Person We Assist when receiving services from the Society.

38. Individuals will be asked to consent to the collection, use and disclosure of their Personal Information, in a language and a mode which they can understand, in accordance with the terms of the applicable Privacy Collection Statement. Due to the varied nature of the services provided by the Society, individual Directorates must develop and maintain Privacy Collection Statements and consent forms which are appropriate in the particular circumstances, and which have been approved by the Privacy Officer. To assist in the development of such forms, a template has been attached to this Policy as a tool (**Appendix 2)**, which may be adapted as required for the particular information collection. All such forms must be finalised in consultation with the Privacy Officer.

Anonymity

39. As part of its commitment to open and transparent management of Personal Information, the Society will advise individuals when it is possible to interact anonymously or by using a pseudonym. For example, if an individual makes a complaint or a general enquiry, a name will not be required unless the individual chooses to provide it.

How the Society holds Personal Information

40. The Society will take reasonable steps to ensure that Personal Information collected, stored, used and disclosed by it is accurate, complete and up-to-date. To ensure this the Society will:

- aim to record information in a consistent format;
- where necessary and/or possible, confirm the accuracy of the information collected from a third party or a public source;
- promptly add updated or new Personal Information to existing records; and
- review the quality of Personal Information before it is used or disclosed.

41. Under Australian Privacy Laws, the Society is responsible for taking reasonable steps to protect Personal Information that it holds from misuse, interference or loss, or unauthorised access, modification or disclosure.

42. The Society holds Personal Information in secure environments electronically in document management systems or repositories, or hard copy (paper) form. (Refer to paragraph 73 below regarding the requirements for security of information.)

43. The Society may use other organisations to assist with data storage, management and other related services. Such organisations may be related to the Society or may be third party suppliers which the Society has contracted to provide systems, software or services which hold Personal Information.

44. Contracts with third party suppliers must encompass appropriate obligations and requirements in relation to the security and privacy of Personal Information. Managers who are responsible for contracts with third parties who assist the Society with the storage, management or processing of Personal Information should liaise with Legal Services and Information & Communications Technology (ICT) to ensure that appropriate contractual protections are in place and that the third party's products and services meet the Society's requirements in relation to information security. (Refer to paragraph 60 below, in relation to the transfer of Personal Information outside of Australia.)

When Personal Information requested is not provided

45. Individuals can decline to provide Personal Information to the Society. However, if the Personal Information requested is not provided, the Society may not be able to:

- provide the requested services (or information about those services), either to the same standard or at all
- engage an individual as a volunteer, member, employee or contractor
- employ or enter into a contract with an individual
- meet funding, professional and legal obligations;
- respond to a complaint, or
- tailor the content of our websites, which might impact the experience of our websites.

Use and disclosure of Personal Information

Permitted use and disclosure

46. Under Australian Privacy Laws, the Society can only use or disclose Personal Information for a purpose for which it was collected (known as the "primary purpose") or for a secondary purpose where certain exceptions apply. An example of such an exception is where the individual has consented to the secondary use or disclosure.

47. In general, the Society only uses or discloses Personal Information for the primary purposes for which the information was collected (as described in the relevant Privacy Collection Statement) and otherwise in accordance with the individuals consent.

48. Guidance should be sought from the Privacy Officer prior to any other proposed use or disclosure, to ensure that it is permitted under Australian Privacy Laws. Certain limited exceptions apply where Personal Information is required to be disclosed by law or under a court / tribunal order (e.g., in response to a subpoena), or reasonably necessary for enforcement activities conducted by an enforcement body (e.g., in response to a written request from NSW or Federal Police). Society Personnel should assess each proposed disclosure on its particular circumstances and with the assistance of the Privacy Officer.

49. In accordance with the Society's publicly available Privacy Policy, the applicable Privacy Collection Statement and the individual's consent, Personal Information may be disclosed to certain third parties including:

- contractors
- suppliers and other service providers, including those who assist in fundraising strategy, activities, and analysis
- funders
- regulators, and
- other charities or not-for-profit organisations.

Disclosure to suppliers and service providers

50. It may be necessary to disclose Personal Information to third parties who are contracted to provide products and services which assist the Society to carry out its work. Third party suppliers are required to comply with confidentiality requirements when handling Personal Information and the Society also seeks to ensure that its suppliers have appropriate measures in place to safeguard the security of Personal Information held by them.

51. Managers, who are responsible for contracts with third parties to whom Personal Information may be disclosed, should liaise with Procurement and ICT or Legal Services in advance of contract execution, to ensure that appropriate contractual protections are in place and that the third party's products and services meet the Society's requirements in relation to information security. Please refer to the Procurement Policy for further guidance on contracting with third parties.

Disclosure to other charities

52. From time to time the Society provides some Personal Information to other charities and data co-ops, based in Australia and subject to Australian privacy laws, to increase its donor base.

Disclosure when services are provided to an individual

53. If the Society provides services to an individual, their Personal Information, including Health information and Sensitive Information may be disclosed to:

- the individual's authorised representative
- other non-government agencies or government agencies with which the Society has a partnership for the delivery of its services
- members of a health treatment team (including other health service providers involved in diagnosis, care and treatment) to the extent necessary to improve or maintain their health or manage a disability
- employees, volunteers, contractors, suppliers or service providers for the purposes of providing the service
- external professional organisations or individuals in circumstances where a Society employee, intern or volunteer is subject to external professional supervision or peer review, and
- other individuals or organisations for any authorised purpose with the individual's express consent.

Dealing with requests for disclosure

54. The Society will not disclose an individual's Personal Information to another party if the individual explicitly denies consent for the disclosure, except as required by law.

55. Staff should contact the Privacy Officer or Legal Services for assistance with managing a disclosure request received from a third party, such as a court/tribunal or a law enforcement agency. Any disclosure request which is received from a third party should be made in writing when possible and practical. If it is not possible or practical to obtain a disclosure request in writing, then this will be recorded by the Society.

56. The Society will comply with disclosure requests regarding information held about an individual to comply with legal obligations, including:

- to a court, tribunal or commission of inquiry pursuant to an order or subpoena;
- information relating to the safety, welfare and wellbeing of a child or young person under Chapter 16A of the *Children and Young Persons (Care and Protection) Act 1998;* and
- where there is a serious or imminent threat to the life or health of the individual concerned or another person.

57. While complying with relevant laws which require the disclosure of Personal Information, the Society will only disclose such information as is necessary and required.

Disclosure of Personal Information to an overseas person / entity

58. The Society is a global organisation with affiliates that operate all over the world. From time to time, the Society also utilises third party suppliers who are located outside of Australia (e.g. USA, UK and Canada) and may disclose Personal Information to those suppliers to receive products or services.

59. Under Australian Privacy Laws, the Society is responsible for ensuring that any disclosure of Personal Information to third parties overseas, including to the Society's own overseas affiliates, is done in compliance with those laws. This includes taking reasonable steps to ensure that the overseas recipient does not breach the Australian Privacy Principles in relation to the information transferred.

60. Managers, who are responsible for contracts or arrangements with third parties which involve the transfer of Personal Information outside of Australia, should liaise with Procurement and ICT or Legal Services to ensure that appropriate contractual protections are in place and that the third party's products and services meet the Society's requirements in relation to information security. Please refer to the Procurement Policy for further guidance on contracting with third parties.

Use of government assigned identifiers

61. Under the APPs, the Society is not permitted to use any government assigned identifier, such as an individual's Tax File Number, Centrelink Customer Reference Number (CRN) or Medicare Number, as a primary form of identification.

62. Accordingly, Government assigned identifiers must only be collected where reasonably necessary to provide support to the relevant individual (e.g., where the Society is advocating with a Government agency on the individual's behalf or checking eligibility for concessions, rebates and services, with the individual's consent).

63. The Society's use of an individual's Government assigned identifier must be strictly limited to the purpose for which it was collected, and no other purpose.

The Society's website and online presence

Interaction with the Society via social media

64. The Society uses social media platforms such as Facebook to facilitate its business activities and functions and to post information about events and activities. Individuals who interact with the Society through those services are responsible for reviewing and accepting their privacy policies prior to interacting with the Society. Some of these platforms may use cloud-based data storage services and / or store information overseas. The privacy laws of those countries may not provide the same level of protection as Australian privacy laws. Individuals providing information to the

Society on these platforms may not be able to seek redress against these services under Australian privacy laws and may not be able to seek redress overseas.

The Society's website

65. Where the Society's public website (www.vinnies.org.au/nsw) (Website) allows individuals to make comments, give feedback or make a credit card payment, the Society may collect email addresses and other contact details. The Society may use email addresses provided to respond to feedback and, on occasion, to make direct contact for surveying purposes and ongoing communication.

66. If individuals visit the Society's Website to read, browse or download information, information such as the date and time of the visit to the Website, the pages accessed and any information downloaded may be recorded and used for statistical, reporting and Website administration, security and maintenance purposes. The Society may log IP addresses (that is, the electronic addresses of computers connected to the internet) to analyse trends, administer and secure the Website, track users' movements, and gather broad demographic information.

67. The Website collects limited generic user information to identify generic user behaviours such as webpages visited and popular content. The Website may use 'cookies' (small summary files containing an ID number unique to the visitor's computer). Cookies allow the Society's system to identify and interact more effectively with other devices. They help the Society to maintain the continuity of the browsing session, remember the visitor's details and preferences if they return, and to measure traffic patterns to determine which areas of our Website have been visited so that we can improve our services. These cookies do not collect Personal Information. Individuals can configure the web browser software to reject cookies, however some parts of the Website may not have full functionality in that case.

68. The Society engages external data aggregators including Facebook and Google Analytics to identify individuals who may be interested in Society campaigns and activities, based on their usage of the Website. The Society uses Google Analytics to inform and optimise content based on an individual's past visits to the Website. Google Analytics informs the Society how visitors use the Website based on their browsing habits, so that the Society can improve the Website, and make it easier to find information. Google also receives this information as individuals browse the Website and other websites on the Google Display Network using Remarketing. Individuals can opt-out of customised Google Display Network services and Google Analytics for Display Advertising using ad settings and can use the Google Analytics Opt-out Browser Add-on to not be tracked into Google Analytics.

69. The Website may contain links to other sites operated by third parties. Third party websites are responsible for informing visitors about their own privacy practices and the Society is not responsible for the privacy practices or policies of those sites.

Email communications

70. When the Society sends emails or other electronic messages, it may record where the message was opened and what links were clicked to better understand what information is of interest to the viewer.

Information in transit

71. The Society is subject to laws requiring it to protect the security of Personal Information once it comes into its possession. However, any Personal Information sent through the Website or other

electronic means may be insecure in transit, particularly where no encryption is used (for example email or standard HTTP).

72. Despite all precautions taken by the Society to protect Personal Information, because the Website is linked to the Internet, no assurance can be given regarding the security of any transmission of information individuals communicate online. The Society also cannot guarantee that information supplied will not be intercepted while being transmitted over the internet. Accordingly, any Personal Information or other information transmitted to the Society online is transmitted at the individual's own risk.

Storage and security of Personal Information

73. Under the APPs, the Society is responsible for taking reasonable steps to ensure that Personal Information is protected from misuse, interference, loss and unauthorised access, modification or disclosure. Personal Information held by the Society in electronic form must be stored in electronic databases or systems that require passwords and logins and otherwise meet the Society's information security requirements. ICT is responsible for maintaining appropriate controls for the secure management of Personal Information on the Society's technology systems. Individual Directorates are responsible for developing and maintaining appropriate physical security controls in relation to the secure storage of hard copy documents.

74. The Society will maintain restricted access systems and tools, where only appropriate Society Personnel have access to files containing Personal Information.

75. The Society protects information held from both internal and external threats by:

- regularly assessing the risk of misuse, interference, loss and unauthorised access, modification or disclosure of that information
- taking measures to address those risks, for example, by keeping a record (audit trail) of when someone has added, changed or deleted Personal Information held by the Society electronically
- maintaining electronic security of Society premises and information systems, including password protection for electronic files, protection of internal network and databases using firewalls, intrusion detection and other technologies.

Destruction and de-identification of Personal Information

76. When Personal Information is no longer needed by the Society, there is an obligation under the APPs to take reasonable steps to destroy or de-identify the information, unless required to be retained by law or a court / tribunal order.

77. The Society will take reasonable steps to ensure that Personal Information relating to individuals is de-identified when such information is required for reporting or other statistical purposes.

78. The Society's ***Records Management Policy*** provides further information on the retention, disposal and destruction of the Society's records, including records which incorporate Personal Information. The Society is also required to comply with requirements under the *Archives Act* 1983 (Cth) to protect Personal Information it holds.

79. Generally, the Society is required to keep records for a minimum of seven years from the date it was last accessed or until the person has reached 25 years of age, whichever is longer.

Accessing and correcting Personal Information

80. The APPs require that where the Society holds Personal Information about an individual, that individual must be given access to their Personal Information on request.

81. Under the APPs, the Society is also required to take reasonable steps to correct Personal Information to ensure that it remains accurate, up-to-date, complete, relevant and not misleading. This requirement applies when the Society itself identifies that the information is incorrect, or where the relevant individual requests correction of their Personal Information.

Requests for access

82. An individual or their Authorised Representative may request formal access to their Personal Information held by the Society at any time by making a written request to the Privacy Officer, St Vincent de Paul Society NSW, PO Box 5, Petersham NSW 2049 or by email at privacy@vinnies.org.au.

83. All requests for access to Personal Information are handled by the Society's Privacy Officer.

84. After the Society has established the identity of the individual (by requesting appropriate personal identification) and if applicable, the requisite authority of their Authorised Representative, the Society will usually make the requested information available for inspection within 28 days upon receipt of the request for access. Some services may have additional requirements relating to access (such as requiring individuals to view files in person with Society Personnel present to provide additional support or information).

85. The Society may refuse access where it reasonably believes that granting access would pose a serious threat to the life, health or safety of an individual or to public health and safety, have an unreasonable impact on the privacy of another individual or would result in a breach of confidentiality. Where the Society refuses access, it will give written reasons. Where the Society refuses access to Personal Information on the ground that it would present a serious threat to an individual's life or health, an individual may request the Society to provide access through an intermediary (such as a treating medical practitioner) who would consider whether access should be provided.

Requests for correction

86. Individuals or their Authorised Representative can make a request for correction of Personal Information in writing, if they believe the information held by the Society is inaccurate, out-of-date, misleading or incomplete.

87. The request will be treated confidentially. In responding to the request, the Society will:

- consider if the information requires amendment
- if it agrees that the information requires amendment, correct the information as soon as practicable and notify the individual that the changes have been made
- if it does not agree that there are grounds for amendment, provide notification in writing of the reasons for declining the request. The Society will also provide notification of any available avenues for review of the refusal and will add a note to the Personal Information indicating that the individual has requested that the information is amended.

Privacy and data breaches

88. Despite the Society's best efforts to protect and safeguard individuals' privacy, information data breaches may occur including:

    - unauthorised access (including Society Personnel, contractors or external third parties such as by hacking, phishing etc.)
    - unauthorised disclosure (whether intentional or unintentional through system fault or human error – for example, an employee accidentally sends Personal Information of individuals accessing a particular service to the wrong email address)
    - loss or theft (for example, hardcopies of documents, electronic devices and storage devices being misplaced or stolen).

89. The Society has developed a ***Data Breach Response Plan*** which sets out the roles and responsibilities involved in managing a data breach and a detailed step by step plan for dealing with suspected or actual data breaches. Please refer to that Plan for further guidance, in addition to the general information on data breaches which is provided below.

90. When a data breach or suspected data breach is first detected, staff responsible must make all efforts necessary to contain the breach and mitigate the serious harm.

91. If there is suspicion that a data breach has occurred (but no reasonable grounds to believe it has), the Executive Manager responsible for the area concerned must be notified immediately and staff responsible must conduct an assessment within 30 days to determine whether the breach has occurred. If, during the investigation it is revealed that the 30-day timeframe is not feasible (e.g. given the complexity or sheer scale of the investigation) an application for an extension can be made to the OAIC. If it becomes apparent that a data breach has occurred, then the steps outlined below (paragraphs 92 - 99) should be followed.

92. The Executive Director of the relevant area and the Privacy Officer must be informed immediately of any actual data breach and the circumstances surrounding it. Management will then consult with the Privacy Officer, and Legal Services as appropriate, to determine appropriate next steps in relation to the data breach, including making a determination as to whether the breach comprises an Eligible Data Breach which requires notification to the OAIC and persons affected by the breach (refer paragraph 93 below).

93. The Society must notify the OAIC and affected individuals of any Eligible Data Breach. An Eligible Data Breach occurs when:

    - there is unauthorised access to, or unauthorised disclosure of, Personal Information, or loss of Personal Information, that an organisation holds
    - this is likely to result in serious harm to one or more individuals, and
    - the organisation hasn't been able to prevent the likely risk of serious harm.

94. In these circumstances the Society must notify the OAIC and the affected individuals of certain matters, including a description of the Eligible Data Breach, the kinds of information concerned (for example, whether health records are included) and recommended steps individuals can take in response to the breach.

95. The Privacy Officer must be informed whenever the Society (or a third-party supplier) experiences a data breach, so that they may assist with the investigation and assessment of the incident and consider the regulatory reporting requirements.

96. The Privacy Officer is responsible for making any report to the OAIC in relation to an Eligible Data Breach.

97. When notifying individuals of an Eligible Data Breach, the Society will, depending on the most appropriate course, either notify all affected individuals; or notify only those individuals at risk of serious harm; or if those options are not feasible, publish a Notifiable Data Breach statement on the Website and publicise that statement.

98. Where the Society is required to also report the breach to other enforcement agencies, it will take reasonable steps to inform individuals concerned.

99. If there is a data breach concerning more than one entity (i.e. the data breach relates to Personal Information held by a third-party supplier as service provider to the Society), only one of the entities is required to notify and prepare a statement. The Society's Privacy Officer will consider, in consultation with Legal Services and taking into consideration any applicable contractual obligations, which entity will be responsible for notifying the OAIC. In general, the entity with the most direct relationship with the individuals affected by the data breach should carry out the notification.

Complaining about a breach of privacy

100. An individual, or their Authorised Representative, with any questions or concerns regarding a possible privacy breach, should contact the Society's Privacy Officer who will discuss the concerns and outline options for resolution.

101. The contact details for the Society's Privacy Officer are as follows:

- PO Box 5, Petersham NSW 2049
- email to privacy@vinnies.org.au
- telephone (02) 9568 0262

102. The Society will provide an accessible procedure to receive and resolve complaints in a timely manner that is procedurally fair, without reprisal for the person making the complaint.

103. Where an individual does not have an Authorised Representative and requires support to make a complaint, the Society will ensure that appropriate support and assistance is provided to them to do so.

104. The Society will aim to resolve complaints in a timely, satisfactory, fair and transparent manner in accordance with the Society's ***Feedback and Complaints Policy***.

105. If an individual is not satisfied with the result of their complaint, depending on the nature of the complaint, they or their Authorised Representative may make a complaint to the OAIC, whose contact details are as follows:

- OAIC
  GPO Box 5218
  Sydney NSW 2001
  Fax +61 2 9284 9666
  Email to enquiries@oaic.gov.au

Roles and responsibilities

106. The Executive Director, Governance, Legal and Risk is responsible for maintaining the currency of this Privacy Management Policy.

107. Each Executive Director and the Chief Financial Officer is responsible for managing legal compliance obligations in their directorates and for promoting, monitoring and upholding a positive compliance culture and identifying the need to engage support and/or training for staff and volunteers to implement the policy.

108. The Executive Director, Membership, Volunteers and Regional Operations is responsible for managing the legal compliance obligations of members and volunteers and for identifying the need to engage support and/or training to implement this Policy in their area.

109. The Society shall provide training and send staff, members and volunteers regular reminders regarding information security and their privacy responsibilities.

Review

110. This Policy will be reviewed every three (3) years or on a needs basis as required to align with legislative, operational or practice changes.

111. The effectiveness of the operation and socialisation of this policy is to be evaluated and reviewed by the Executive Director, Governance, Legal and Risk, in consultation with the Privacy Officer.

Further assistance

112. Society Personnel should speak with their Manager regarding any questions about the implementation of this policy. They may also contact the Executive Director, Corporate Services to provide feedback on this policy.

113. Questions regarding the application of this Policy, or requests for assistance in relation to the development of any documentation or materials in connection with it (e.g. a Privacy Collection Statement) should be directed to the Privacy Officer in the first instance::

    Phone: (02) 9568 0262
    Email: privacy@vinnies.org.au
    Post: PO Box 5 Petersham NSW 2049
    Visit: 2C West St Lewisham NSW 2049

References

114. Legislation, regulations and guides relevant to this policy include:

- *Privacy Act 1988* (Cth) including the *Australian Privacy Principles*
- *Health Records and Information Privacy Act 2002* (NSW)
- *National Disability Insurance Scheme (Complaints Management and Resolution) Rules 2018*
- *Children and Young Persons (Care and Protection) Act 1998* (NSW)
- *National Disability Insurance Scheme Act 2013* (Cth), Chapter 4 Part 2
- *Workplace Surveillance Act 2005*

Approval and amendment history

Version	Approval authority	Date	Amendment summary
Version 1	SVDP Society NSW Board	19 August 2015	N/A
Doc #PO2019-02	SVDP Society NSW Board	Board endorsement 5 June 2019	Insertion of section on Data Breaches to ensure compliance with changes to legislation regarding the Notifiable Data Breaches (NDB) Scheme that came into effect on February 22, 2018. Updating policy to ensure compliance with NDIS legislation and Guidelines. Amended review period to annual review to align with recommendations of Deloitte Privacy and Security Assessment (October 2017).
Doc #PO2019-02 Version 2	Executive Director Corporate Services	27 July 2020	Updated policy owner and responsibilities to align with organisational structure changes
Doc Policy PO2023-02	SVDP NSW Board of Directors State Council	1 June 2023 17 June 2023	New policy. Privacy Policy rescinded – replaced with Privacy Policy PO2023-058 (external) and Privacy Management Policy PO2023-02 (internal).

Appendix 1: Definitions

Australian Privacy Laws	Federal and State / Territory legislation which governs the use of Personal Information, including • the Privacy Act including the Australian Privacy Principles; • the *Health Records and Information Privacy Act 2002* (NSW); and any other laws that protect specific types of Personal Information in service delivery, for example, to children, older people and people with disabilities.
Australian Privacy Principles (APPs)	The Australian Privacy Principles contained in Schedule 1 of the Privacy Act
Authorised Representative	A person authorised in writing by an individual to act on their behalf.
Chapter 16A information	Information relating to a child or young person's safety, welfare or wellbeing that Chapter 16A of the *Children and Young Persons (Care and Protection) Act 1998* (NSW) allows prescribed bodies to exchange without consent, where necessary, despite other laws that prohibit disclosure of information such as the *Privacy Act*.
Eligible Data Breach	An eligible data breach occurs when: 1. there is unauthorised access to or unauthorised disclosure of Personal Information, or a loss of Personal Information, that an entity holds; 2. this is likely to result in serious harm to one or more individuals, and 3. the entity has not been able to prevent the likely risk of serious harm with remedial action.
Health Information	Any Personal Information about your health or disability. It includes information or opinion about an individual's illness, injury or disability. For example, information about any health service that has been or is to be provided to an individual, any Personal Information collected to provide or in providing a health service, information collected in connection with a donation or intended donation of body parts, organs or body substances, genetic information, specialist reports and test results, dental records, prescriptions and other pharmaceutical purchases, appointment and billing details and healthcare identifiers.
OAIC	Office of the Australian Information Commissioner
Personal Information	Information or an opinion about an identified individual, or an individual who is reasonably identifiable: a. whether the information or opinion is true or not; and b. whether the information or opinion is recorded in a material form or not Examples of Personal Information include an individual's name, address, telephone number, email address, date of birth, signature,

	salary and banking details. Personal Information includes Health Information and Sensitive Information.
Privacy Act	Privacy Act 1988 (Cth)
Privacy Collection Statement	Notification provided to an individual under APP5, which sets out the following matters in relation to the collection of their Personal Information: • the identity and contact details of the entity collecting the information • if the entity is collecting the information from someone other than the individual, or the individual may not be aware of collection, the fact that the entity has in fact collected the information and the circumstances of that collection • if the collection of the information is required / authorised by law or a court / tribunal order, then the fact that the collection of so required / authorised and details as to the authority • the purposes for which the entity collects the information • the main consequences (if any) if all or some of the information is not collected • any other persons or entities to whom the information may be disclosed • that the Privacy Policy contains further information on how individuals may access and seek correction of their Personal Information • that the Privacy Policy contains more information on how the individual may complain about a breach of privacy and how such complaints will be dealt with • whether the entity is likely to disclose Personal Information to overseas recipients and if so, the countries in which such recipients are likely to be located (if practicable)
Privacy Officer	The Society's Privacy Officer who may be contacted at privacy@vinnies.org.au
Sensitive Information	A type of Personal Information and includes information or an opinion about an individual's • racial or ethnic origin • political opinions or associations • religious or philosophical beliefs • trade union membership or associations • sexual orientation or practices • criminal record • health or genetic information

	• some aspects of biometric information Generally, Sensitive Information has a higher level of privacy protection than other Personal Information.
Subpoena	A legal document issued by a court at the request of a party to a case. It requires a person to produce documents and/or give evidence. Failure to comply may result in a charge of contempt of court.
Society Personnel	Any person (or group of people) engaged by the Society to assist in its works. This includes members, volunteers, employees, contractors and consultants.
Whistleblower Hotline and website reporting	A confidential telephone line (1300 304 550) and email facility (vinniesnsw@stopline.com.au) managed and staffed by an independent third party for advice and for making legitimate allegations of wrongdoing.

Appendix 2: Template Privacy Collection Statement and Consent Form

Acknowledgement and Consents

I acknowledge that the Society has provided me with this privacy collection statement, and that:

- I have read and understood this statement
- I can access a copy of this statement [*Insert website address*], or
- I can contact the Society's Privacy Officer to discuss any queries or concerns I have, or any complaint I would like to make, about the handling of personal information by the Society by email: privacy@vinnies.org.au or phone: 02 9568 0262.

In making this acknowledgement, I consent to the Society [*amend list below as appropriate*]:

- collecting sensitive information about me
- collecting sensitive information about minors who I am a legal guardian or parent of (to the extent that I volunteer such sensitive information)
- using and disclosing personal information for funding and fundraising purposes
- using and disclosing personal information for reporting and statistical purposes [*Once determined what information will be reported under its funding arrangements, then consider whether more detail is required here and in statement below to explain this to clients for proper informed consent*]
- using and disclosing personal information for responding to media requests, and
- disclosing personal information about me to other members of my household if they are a Society client or become one in the future (unless you have expressly told us not to do so) and using and disclosing personal information about me in connection with the Society's dealings with those other members of my household (unless you have expressly told us not to do so).

Introduction

The St Vincent de Paul Society NSW ACN 161 127 340 and its related entities (the **Society**, **us**, **we**, **our**) recognise and value the protection of your personal information.

This is the Society's privacy collection statement for [clients and prospective clients of the Society. If you enquire about our services, or become a client of the Society,] then the Society will collect and handle personal information as described in this statement.

Sometimes another policy or privacy collection statement may apply instead of, or in addition to, this statement. If that's the case we will let you know and direct you to that additional information.

By using our website at www.vinnies.org.au/nsw (**Website**), or otherwise engaging with us, you acknowledge that we may handle the personal information we collect in connection with our dealings with you in accordance with this privacy collection statement.

Collection of Personal Information *[review and confirm if any other types of collections are missing, in which case these should be added, and plus other changes as required*]

The nature of the personal information we collect about you will depend on the reason for your dealings with us. Generally, we collect personal information such as your name, title, contact details (address, phone, e-mail address), and depending on our dealings with you we may also collect other information including gender, languages spoken, health information, household and living circumstances information, financial information, and other personal and sensitive information. For example:

- where you engage us to assist you with any NDIS, Services Australia or other personal management services, we may collect relevant identification numbers, and information about your health, your financial situation, living situation, your employment history, your education history and other information that is required to assist with such services;
- where you participate in or use any of our programs such as [Insert], we may collect information about your health, your financial situation, your financial situation, living situation, your employment history, your education history and other information that is required to assist with such services;
- if you participate in surveys and other types of research we may collect information about your health or as other information as required for the particular survey or research;
- that is necessary for us to fulfill our reporting obligations to regulatory authorities agencies, including any mandatory reporting obligations, and any reporting obligations relating to our funding agreements with government; and
- other information to comply with our obligations as permitted or as otherwise required by law.

Where you provide us with any sensitive information, we assume you consent to our collection of such information unless you tell us otherwise at the time of collection of the information. We will generally not otherwise collect sensitive information about you unless the collection is otherwise authorised or required by law.

Collection of Personal Information about others *[delete if not applicable]*

If you provide us with personal information about your dependents, domestic partners, household members or others, you represent that, and we collect the personal information on the basis that, those individuals agree that we can collect and handle their personal information in accordance with this privacy collection statement (and that where they are under the age of 18 years, that their parent or legal guardian agrees).

How we collect personal information *[check the list below and amend as appropriate]*

We collect personal information about you, when you engage with us, for example:

- by attending one of our conferences to enquire about or to access services;
- by contacting us by telephone, email or other means;
- when we attend your home to provide our services;
- when we contact other agencies or organisations in the course of providing advocacy and support services to you;
- when you attend events or services provided by us;
- if you participate in surveys and other types of research;
- if you subscribe to our mailing lists; and

- other situations where you would reasonably expect information to be collected.

We may in some circumstances collect personal information about you from third parties or other sources. These may include your parents or legal guardian, and other household members, where they engage in the activities described above. These circumstances may also include where you have told us to deal with your authorised representative, from government agencies or other organisations if we advocate to them on your behalf, or from partner and referring agencies where required for us to provide the relevant assistance.

Generally, if we are unable to collect the personal information we require then we may not be able to provide you with the products and services you seek. If the information provided is incorrect or incomplete, this may also prevent, limit or otherwise affect our ability to provide our products or services to you.

Why we collect, use and disclose personal information *[check the list below and amend as appropriate]*

We collect, use and disclose your personal information for the following primary purposes (and other related purposes that you would reasonably expect):

- to respond to your enquiries,
- to enable us to provide our services to you, your dependents and/or other members of your household,
- to enable participation in one of our programs by you, your dependents and/or other members of your household,
- to provide you with advocacy services where we assist you in your dealings with government agencies and/or other organisations,
- to comply with our reporting obligations (such as mandatory reporting) and otherwise in our dealings with regulatory authorities and government agencies, and
- for reporting and statistical purposes, including reporting to government agencies under our funding agreements,
- to respond to media requests,
- for our internal business purposes such as to obtain feedback, conduct surveys, planning future product and service delivery, funding and fundraising purposes, other research and reporting, auditing, promotional and marketing, and compliance with our legal obligations, and
- for other purposes with your consent or as otherwise required or permitted by law.

We may exchange your personal information with our related entities. We may also disclose your personal information to our agents, contractors, service providers and partner organisations for the purposes set out above, and for the purposes of those parties providing services to us or performing business services or functions on our behalf (for example, our technology service providers, marketing service providers, mail distributors, and event organisers).

In addition, we may also disclose your personal information to third parties upon your request, with your consent or as otherwise required or permitted by law, such as your parent or legal guardian, your dependents, your household members, your authorised representative, medical professionals, regulatory authorities. Government agencies and others.

We may also, in the event of a sale, transfer or assignment of the whole or part of the Society's business and/or assets and facilities to a third party, disclose your personal information to that third party for their use in operating the business or assets to be transferred.

Marketing *[delete if not applicable]*

We may use personal information we hold about you for marketing and promotional purposes and we may send you information about other services and programs that may be of interest to you. Our communications to you may be sent in various forms such as by post, email or SMS. You can select your preferred method for receiving these communications or opt-out of receiving these communications altogether. To unsubscribe, use the opt-out mechanism in one of our communications or contact us via the details below.

Further information

If you do not provide us with the personal information that we request, we may be unable to respond to your enquires or provide you with the services you are seeking.

Our Privacy Policy, located on our website at https://www.vinnies.org.au/nsw/about-us/nsw-privacy-policy contains additional information regarding how we handle personal information, including how you may seek access to, or correction of, personal information that we hold about you, and how you may make a complaint if you believe we have handled your personal information in a way that breaches our privacy obligations. If you would like further information, please contact us by email at privacy@vinnies.org.au or by mail at PO Box 5, Petersham, NSW 2049.

Nothing in this collection statement restricts the Society's ability to handle personal information in a manner otherwise consistent with the privacy laws.

[Client] acknowledgment and consent

Name:	Email:
Phone:	Type of information: Personal/ Health/Sensitive *(Please circle all that apply)*

In completing this form and signing it, you give us permission to collect, record, store and use your personal information on the terms outlined in this privacy collection statement.

Name:_____	Authorised Person (if applicable):_____
Signature:_____	Authorised Person Signature:_____
Date: ___/___/_____	Date: ___/___/_____
Name:_____	Witness Name:_____
Signature:_____	Witness Signature:_____
Date: ___/___/_____	Date:___/___/___