



# Records Management Policy

Document number: PO2020-022

*Version 3*

## Approval

Policy owner	Executive Director, Corporate Services		
Approved by	Executive Leadership Team State Council		
Date approved	ELT: 29.04.2020 SC: 19.06.2021	Review date	29.04.022

## Purpose

1. This Policy establishes the principles for the creation, capture, control, use, maintenance, storage, retention, disposal and destruction of the Society's records.
2. This Policy assists the St Vincent de Paul Society NSW (Society) to ensure that proper and efficient record management practices are in place and it meets its legislative and contractual obligations to manage records and information appropriately.
3. The use of effective records management practices:
  - reduces the costs of records storage
  - decreases the time taken to locate records
  - mitigates the risks arising from unmanaged destruction of records, and
  - mitigates against inadvertently keeping records that should be destroyed.<sup>1</sup>

## Scope

4. This policy applies to all **Society Personnel** working in any capacity in the Society including all members, volunteers, employees, contractors and office holders.
5. This policy uses the term '**Record/s**' to refer to all the Society's documents, information and data stored by any means including copies and extracts. A more detailed definition is in Appendix 1.

Records include:

- written documents
- printed documents, including photographs
- electronic records (i.e. email, recordings, business or Society **Approved Information Systems** (e.g. Microsoft Teams/SharePoint and other electronic files)
- anything from which sounds, images or writings can be reproduced with or without the aid of anything else.

This policy relates to all types of records maintained by the Society, including:

- all recorded information and files pertaining to people we assist
  - records of meetings of governance bodies
  - financial and legal records
  - personnel files
  - property and administrative records
  - records of historical or archival significance.
6. This policy sets out record management protocols for the different categories of records (temporary, final and permanent) and includes the creation, capture, control, use, maintenance, storage, retention, disposal and **destruction**.
  7. This policy should be read in conjunction with the Privacy Policy. The Privacy Policy outlines the Society's privacy practices, including how:

---

<https://www.records.nsw.gov.au/recordkeeping/advice/retention-and-disposal>

- Society Personnel collect and manage personal information
  - Society Personnel and people we assist may access and, if required, correct records containing their personal information.
8. This policy does not cover Records whose management and access is specifically mandated by a contractual or funding agreement. In these circumstances, the contract or funding agreement will contain the records management policy and procedures specific to that agreement.

## Related policies and procedures

9. Related policies and procedures include:
- Acceptable Use of Technology Policy
  - Code of Conduct for Members, Volunteers and Employees
  - Conflict of Interest Policy
  - Feedback and Complaints Policy
  - Information Security Policy
  - Privacy Policy
  - Safeguarding Children and Young People Policy.

## Policy principles

10. The Society recognises the importance of managing its documents in an effective and efficient manner that is consistent with ethical, legal, and regulatory requirements.
11. The Society is committed to the permanent preservation of records of historical or archival significance.
12. Society Personnel must not make inappropriate use of information obtained through their position in the Society. Further information regarding inappropriate use of information can be found in the Conflict of Interest Policy and Acceptable Use of Technology Policy.
13. A breach of the Records Management Policy may result in disciplinary action and in some circumstances may include prosecution.
14. Records management requirements must form an essential component of the development, implementation or revision of business information systems and their related processes.
15. The Society must retain all records, in accordance with the Records Management Policy and Records Retention Schedule. In practice, the majority of records will be retained for seven years. A longer time period may be required where:
- it is stipulated in Commonwealth or State Government Funding agreements
  - allegations of abuse and neglect and reports concerning the safeguarding of children and young people, and other vulnerable people
  - adoption records
  - if the Society is involved in litigation or it is anticipated that litigation may proceed
  - the Society deems it appropriate or necessary to maintain records for more than seven years, such as decisions by governance bodies.

16. To ensure that the Society is compliant with the *Privacy Act*, Society Personnel are given access to records and information on an as needs basis and must ensure that records are not used for unintended purposes.
17. Records and information are captured, managed and used in the most efficient and appropriate format, with a preference for digital records where possible.

### Creation of records

18. The ongoing creation of Records is necessary to provide accurate information of decisions and operations.
19. A Record is generated when information is created (internally) or received (from external or other sources) and maintained as evidence of the Society's activities, decisions and operations.
20. The Society's preference is for the creation and maintenance of digital records where possible.
21. Records must be created and stored in the Society's Approved Information Systems, i.e. Microsoft Teams/SharePoint. Until a Society wide classification system is created, each Directorate should adopt a classification system that facilitates easy access and retrieval, and version control of records.

### Storage of records

22. Where physical records exist, these must be stored in an appropriate secure location that is accessible to appropriate Society Personnel with authority to access the records.
23. Where the physical record is of a confidential nature, such as files relating to personnel, membership, people we assist, litigation or legal advice and safeguarding children and young people, they need to be securely stored and accessible to only authorised Society Personnel.
24. Where a physical record has been digitized the original may be disposed of securely.
25. Electronic records must be stored on the Society's approved information systems.
26. Email applications and email archives are not Approved Information Systems. Where an email comprises a record (evidence of the Society's activities and decisions) the email, and any relevant attachments, should be incorporated into the Society's Approved Business Systems (i.e. Microsoft Teams/SharePoint) for records storage and retention purposes.
27. Society Personnel must use Microsoft Teams/SharePoint to store records where available. In areas where Microsoft Teams/SharePoint is not available, other Society approved systems that allow team access can be used. Dropbox and Google Drive are not approved systems.
28. Local network shared drives (e.g. the S drive); personal folders and external storage media must *not* be used for the storage of records.
29. For information about the protection of **Society Information** and the Society's Information Security Management System (ISMS), please refer to the Information Security Policy.

### Retention, disposal and destruction of records

30. The majority of the Society's records must be kept for a minimum of seven years in line with legislation. There are some exceptions, which require records to be held for other periods or indefinitely. Please refer to the Records Retention Schedule (at Appendix 2) for this information.

31. The Disposal, transfer of physical records to archives or destruction of records must be authorised by the appropriate Executive Director, Chief Financial Officer or Director (apart from the circumstances outlined at paragraph 34 below) and a record of the disposal, transfer to archives or destruction must be maintained as a permanent record.
32. Electronic records may be archived within the Society's Approved Information Systems as part of normal operational practice.
33. The destruction of records includes the destruction of digital records, which may require action across different systems and technologies.
34. The destruction of physical records must be carried out securely, either by shredding or otherwise destroyed in order to make them unreadable.
35. Records relating to current, pending or anticipated litigation must not be destroyed. In these circumstances, Society Personnel must not commence or continue the destruction of relevant records until advised by the Director Legal and Complaints.
36. If the Legal and Complaints team becomes aware of potential litigation, they must advise the relevant Executive Director or Chief Financial Officer immediately so that all relevant records are secured.
37. Records must only be disposed of in accordance with this policy, the Society's Records Retention Schedule (at Appendix 2) and with the consent of the relevant Executive Director or Chief Financial Officer in consultation with the Director of Legal and Complaints (to ensure that records are not relevant to current, pending or anticipated legal proceedings).

## Types of Records

38. For the purposes of this policy there are three primary classes of records:

- temporary
- final
- permanent.

### *Temporary records*

39. Temporary records are all records that have not been completed, including, but not limited to:

- minutes to be typed up in the future
- reminders and to-do lists
- drafts such as internal reports and correspondence
- unsolicited email (including spam) and informal communications such as "with compliments" slips.

40. Temporary records can be destroyed (or permanently deleted) once all final records are collated and reviewed, ensuring the file is complete.

41. Minutes are the final record of decisions taken at a meeting. To avoid confusion about which document forms the record of a meeting, any draft document or notes created to prepare Minutes must be destroyed after the Minutes have been approved.

### *Final Records*

42. Final records are all records that are not superseded by modification or addition, including, but not limited to:

- accounting records, which include records that:
  - correctly record and explain how the society spends or receives its money or other assets (Transactions)
  - correctly record and explain the Society's financial position and performance
  - allow for true and fair financial statements to be prepared and audited or reviewed
- correspondence
- documents sent to any third party
- final memorandums and reports
- minutes of meetings (without Board, Council or Committee authority)

43. Final records, unless specifically advised in this Policy or in the Retention Schedule, are to be disposed of seven (7) years after closing the file.

### *Personnel records*

44. Personnel records are a type of final record and include:

- employee's name and commencement date
- the basis of the employee employment (full or part-time, permanent, temporary or casual)
- employee's rate of pay, gross and net amounts paid, and deductions
- hours of work records
- leave records
- pay records
- superannuation contribution records
- termination records.

45. Personnel records are retained within the Society's electronic record keeping systems

46. Personnel records relating to the recruitment process, interviews and employee qualifications must be retained for a period of seven (7) years from the date the employee concludes their service with the Society.

### *Permanent Records*

47. Permanent records include, but are not limited to:

- adoption records
- any record relating to the actual or alleged abuse of a child or young person under the age of eighteen
- any record relating to the actual or alleged abuse of a young person or vulnerable adult
- any document whose destruction is likely to interfere with the administration of justice
- articles of incorporation and registrations
- audited annual reports and financial statements

- Constitution of any St Vincent de Paul entity
- Operational Records such as policies, procedures, agreements and reports
- minutes of meetings (with Board, Council and Committee authority)
- records relating to the disposal of records.

48.All permanent records must be retained indefinitely.

## Personal information

49.The Society complies with requirements under the Privacy Act 1988 (Cth), Archives Act 1983 (Cth) to protect personal information it holds. Generally, the Society is required to keep a record 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.

50.The Society has a restricted access system in place, which allows only authorised Society Personnel access to personal files.

51.For information on legislative and regulatory compliance required regarding the safe and secure keeping of clients 'personal', 'sensitive' and 'health' information, refer to the Privacy Policy.

## Section 16A Exchange of information

52. Chapter 16A of the Children and Young Persons (Care and Protection) Act 1998 (NSW) allows information to be exchanged between prescribed bodies despite other laws that prohibit or restrict the disclosure of personal information.

53. For information on legislative and regulatory compliance regarding Children and Young People, please refer to the Safeguarding Children and Young People Policy.

## Roles and responsibilities

54.The Executive Director, Corporate Services is responsible for maintaining the currency of this policy.

55.Executive Directors/Chief Financial Officer are responsible for:

- managing legal compliance obligations in their directorate
- promoting, monitoring and upholding a positive compliance culture
- identifying the need to engage support and/or training for Society Personnel to implement the policy.

56.Executive Directors and the Chief Financial Officer must be aware of **Vital Records** within their area of responsibility and must ensure that a plan for Vital Records is included in any **Business Continuity Planning**.

57.The Executive Director Corporate Services is responsible for records relating to employment.

58.The Executive Director Mission and Spirituality is responsible for archives and heritage.

59.The Director Legal and Complaints is responsible for providing advice on whether records may be required for current, pending and anticipated legal proceedings.

60.The Chief Information Officer is responsible for maintaining the Society's information systems, including accessibility, security and backup and ensuring the removal of data from systems in accordance with this policy.

61. Society Personnel are responsible for creating and managing records in accordance with this policy and must:

- comply with this Policy
- comply with the Records Retention Schedule
- comply with the *Privacy Act 1988* (Cth)
- keep records for longer than the prescribed retention period where it is considered possible the records will be required for litigation purposes and document the reasons the records were retained.

## Review

62. This Policy and its implementation will be reviewed every two years, or on an as needs basis as required to align with legislative or practice changes.

## Further assistance

63. Society Personnel should speak with their Manager regarding any questions about the implementation of this Policy.

64. Feedback regarding the implementation of this Policy can be provided to the Executive Director, Corporate Services.

## References

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

- Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth)
- Archives Act 1983 (Cth)
- Australian Charities and Not-for-Profits Commission Act 2012 (Cth)
- Charitable Fundraising Act 1991 (NSW)
- Charitable Fundraising Authority Conditions (NSW)
- Children and Young Persons (Care and Protection Act) 1998 (NSW)
- Corporations Act 2001 (Cth)
- Crimes Act 1900 (NSW)
- Fair Work Act 2009 (Cth)
- Government Record keeping <https://www.records.nsw.gov.au/recordkeeping/>
- Income Tax Assessment Act 1936 (Cth)
- Health Records and Information Privacy Act 2002 (NSW)
- Health Records and Information Privacy Code of Practice 2005 (NSW)
- National Disability Insurance Scheme Act 2013 (Cth)
- National Disability Insurance Scheme Act 2013 (Cth)
- Privacy Act 1988 (Cth), including the Australian Privacy Principles
- Privacy and Personal Information Protection Act 1998 (NSW)
- State Records Act 1988 (NSW)
- ISO 15489 *Records Management*



## Approval and amendment history

<b>Version</b>	<b>Approval authority</b>	<b>Date</b>	<b>Amendment summary</b>
Doc 1	NSW State Council	June 2010	NA
Doc # PO2020- 022	Executive Leadership Team	24 April 2020	Changes to update policy, compliance with privacy legislation.
Doc # PO2020- 022  Version 2	Executive Director Corporate Services	27 July 2020	Updated policy owner and responsibilities to align with organisational structure changes
Doc # PO2020- 022  Version 3	State Council	19 June 2021	Added paragraph 24.

## Appendix 1: Definitions

66. Relevant definitions include:

<b>Approved Information System</b>	An integrated set of components for collecting, storing and processing data for the providing of information, knowledge and digital products whose use is authorised by the Society.
<b>Business Continuity Planning</b>	The process involved in creating a system of prevention and recovery from potential threats to an organisation. The plan ensures that personnel and assets are protected and are able to function quickly in the event of a disaster.
<b>Children and Young People</b>	In this Policy document ‘Children’ means persons aged 0-15, ‘young people’ is any person aged 16-17.
<b>Destruction</b>	Destruction of a record means the physical destruction of paper records, deleting emails, documents or other data from business systems.
<b>Disposal</b>	Disposal of a record means the transfer of its custody or ownership. The transfer of records to another organisation, including government, can constitute disposal where records are not retained by the Society after the transfer. <sup>2</sup>
<b>Health Information</b>	This may include: <ul style="list-style-type: none"> <li>• information about physical, mental health or a disability an individual has had at any time</li> <li>• an individual’s express wishes about future provision of health services</li> <li>• any health service that has been or is to be provided to an individual</li> <li>• any personal information collected to provide or in providing a health service</li> <li>• information collected in connection with a donation or intended donation of body parts, organs or body substances</li> <li>• genetic information that is or could be predictive of health at any time of the individual or a relative of the individual and healthcare identifiers.</li> </ul>
<b>Operational Records</b>	An operational record is any information about the Society’s activities that demonstrate that the Society is compliant with its legal, financial or other obligations.
<b>Personal Information</b>	Information in electronic or hard copy form that either personally identifies, or can be used to reasonably identify, an individual (including their name, address, telephone number, email address, date of birth, signature, salary and banking details). It includes health and sensitive information.

---

<sup>2</sup> Archives Act 1983 (Cth)

<b>Record/s</b>	<p>Record means any document or other source of information compiled, recorded or stored in written form or on film, or by electronic process, or in any other manner or by any other means (<i>State Records Act 1998</i>, Part 1, Preliminary, Section 3(1), Definitions).</p> <p>A record includes any form in which information is stored on a permanent basis or from which information may be reproduced. The <i>Electronic Transactions Act 2000</i> (NSW) and the <i>Electronic Transactions Act 1999</i> (Cth) give validity to electronic documents as a means of storage, in addition to traditional paper or other forms. Therefore, under both NSW and Commonwealth legislation, scanned copies of documents satisfy relevant legislation requirements. The <i>Evidence Act 1995</i> (NSW) also supports these records as being admissible as evidence.</p>
<b>Records Management</b>	Records management is the field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including the process for capturing and maintaining information about business activities and transactions in the form of records. <i>ISO 1549-2001</i>
<b>Sensitive Information</b>	‘sensitive information’ (includes information or opinion about an individual’s racial or ethnic origin, political opinion, religious beliefs, sexual orientation or criminal record, provided the information or opinion otherwise meets the definition of personal information).
<b>Local network shared Drive</b>	A computer drive on a local network that shares files and applications with users in a specific network.
<b>Society Information</b>	All information held by the Society including information used, processed and communicated for the purposes of carrying out Society functions of activities.
<b>Society Personnel</b>	Any person (or group of people) engaged by the Society to assist in its works. This includes members, volunteers, employees, contractors and consultants.
<b>Vital Record</b>	A document, record or file in any format containing information essential to create and organise operations and for the survival of an organisation. Vital Records are necessary to enable the Society to resume operations after an emergency and protect the legal and financial rights of the Society and its stakeholders. Vital Records are those without which the Society could not continue to operate, are irreplaceable or would require significant resources to recreate.
<b>Vulnerable adult</b>	An individual aged 18 years and above who is or may be unable to take care of themselves, or is unable to protect themselves against harm or exploitation by reason of age, illness, trauma or disability, or any other reason.