



P012 - Records Management Policy

1. Purpose

The purpose of this policy is to define the controls needed for the identification, storage, protection, retrieval, retention and disposal of records. Australasian College of Sport and Exercise Physicians (ACSEP) ABN 40 003 200 584 (ACSEP, “the College”) complies with the requirements of Clause 23 of Schedule 1A and the Information Privacy Principles of the *Principles Act 1988 (Cth)* in relation to the collection of information relating to members.

The specific practices, procedures and systems for handling personal information (defined below) are covered by *P004 – Privacy Policy*.

2. Policy-Related Definitions

	Definition
ACSEP	The Australasian College of Sport and Exercise Physicians
Business systems	Automated or manual tools that create, use, manage, or provide access to information, and which are designed to perform a set of functions to meet certain business needs
Disposal	The destruction or deletion of records in or from recordkeeping systems
Members	College Fellows, Registrars, student members, Overseas Trained Specialists, Retired Fellows, CPD Program Members and Committee Members of the College
Personal Information	Includes, but is not limited to: <ol style="list-style-type: none">1. contact information (including name, date of birth, address, phone number and email address)2. financial information (including billing address and payment information such as credit/debit card and bank details)3. personal signatures4. employment details



	<ol style="list-style-type: none"> 5. referee information 6. education and employment history 7. qualifications, training programs and comparability assessment information 8. professional membership such as medical registration numbers, 9. Medical Board or other relevant registration.
Record	Any document or other source of information, in any format or medium, that is compiled, recorded or stored, by electronic process, or in any other manner or by any other means.
Recordkeeping	Creating and maintaining complete, accurate and reliable evidence of business transactions in the form of recorded information.

3. Policy

3.1 Recordkeeping procedures and practices

- The College maintains a records management system which includes this policy, all business systems that function as recordkeeping systems and all College archives. This system is overseen by College governance structures.
- Records made in the course of College activities will be done so in an accurate, authentic, reliable and trustworthy manner.
- College Staff will access records only when they have a business need to do so. Access to records in business systems will be regularly reviewed.
- Only authorized personnel can access records with restricted access requirements (e.g., passwords) and the access rights of such personnel will be regularly reviewed by the College.
- Recordkeeping systems will be maintained and managed for as long as they are needed, and will ensure that records are protected from theft, loss, unauthorised access, and misuse.
- To securely protect records, ACSEP utilises IT protection systems and maintains website security using firewalls. Additionally, ACSEP may store electronic information on remote servers or through contracted agencies in Australia and New Zealand, as permitted by privacy legislation.



- Records generated by outsourced, cloud or similar services used by the College must also abide by the obligations of this policy. Contractual agreements with such services must stipulate what will happen to College records at the expiration of the agreement.
- If a business system used by the College is upgraded or replaced, the records they contain will be migrated to the upgraded or replacement system.
- Records of member information (including personal information, Training Program requirements and any other documentation relevant to their membership) will be kept in electronic copy and be retained for a maximum of 7 years, at which time it will be destroyed or de-identified unless its retention is required or permitted by law.
- All reasonable steps will be taken to protect confidential information, and these protections will be regularly reviewed to ensure they provide an appropriate level of security.
- Records will not be destroyed or disposed of without authorisation.

3.2 Collection, storage, security and disclosure of personal information

- Personal information will generally be
 - collected for a purpose directly related to members; or
 - for any secondary purpose that is related to the primary purpose and for which the member would reasonably expect ACSEP to use the collected information.
- Personal information will not be collected by unlawful or unfair means.
- Where personal information is collected for inclusion in a record or in a generally available publication, ACSEP will take reasonable steps to ensure that, before the information is collected, the member concerned is generally aware of:
 - The purpose for which the information is being collected;
 - If the collection of the information is authorised or required by or under law the fact that the collection of the information is so authorised or required; and
 - With whom the information may be shared.
- Where ACSEP solicits and collects personal information for inclusion in a record or in a generally available publication it will take reasonable steps to ensure that the information collected is relevant to that purpose and is up to date and complete, and the collection of the information does not intrude to an unreasonable extent upon the personal affairs of the member.



- ACSEP will ensure that a member's personal information is kept safe, secure and accessible only to authorised personnel. The College will take reasonable steps to ensure that personal information is protected from misuse, unauthorised access, disclosure, modification or loss.
- ACSEP will not use a person's signature without prior written approval from that individual authorising such use.
- ACSEP will not use a member's personal information without taking reasonable steps to ensure that, having regard to the purpose for which the information is proposed to be used, the information is accurate, up to date and complete.
- ACSEP will not use a member's personal information except for a purpose to which the information is relevant and will ensure to prevent unauthorised use or disclosure of that personal information.
- ACSEP will not disclose a member's personal information to a person, body or agency (other than the individual concerned) unless:
 - The individual concerned is reasonably likely to have been aware that information of that kind is usually passed to that person, body or agency;
 - The individual concerned has consented to the disclosure;
 - ACSEP believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the member or of another person;
 - The disclosure is required or authorised by or under law; or
 - The disclosure is reasonably necessary for the enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue.
- A person, body or agency to whom personal information is disclosed will not use or disclose the information for a purpose other than the purpose for which the information was given to the person.

3.3. Any Staff or College member who becomes aware of a breach or potential breach of this policy must report it as soon as possible to the CEO for appropriate action. In the case that the CEO is the subject of the report, the Chair of the Board should be notified as soon as possible.

3.4 How data should be destroyed and deleted

- In most circumstances, records should be destroyed after its retention period has elapsed and it is no longer required for a business function or to comply with a legal requirement.



- Any Disposal of the record must be lawful and only carried out with the appropriate authorisation. For the avoidance of doubt, records may hold evidentiary value at law. The destruction or prevention of documents from being used as evidence in a legal proceeding is an offence under legislation including, but not limited to, the *Crimes Act 1958* (Vic).

Destruction of Electronic Records Requirements

- The College is responsible for ensuring that reasonable steps are taken to destroy the personal information held in electronic format.
- All personal information should be immediately deleted when no longer required.
- Personal information is considered to be irretrievable when the information can no longer be accessed, and access to the deleted information cannot be given to another entity or staff member.
- Where an individual has instructed the College to irretrievably destroy their personal information, this should include any data backup copies.

Destruction of Hard Copy (Physical) Records Requirements

Hard copy records should not be placed in general waste bins. The process of destroying personal information must be irreversible and therefore destroyed in one of the following manners:

- Shredding
- Secure Disposal Bins
- Burning (not recommended and should only be used as a last resort if there is no environmentally friendly method of destruction available)

3.5 De-identifying personal information requirements

There may be certain circumstances in which the data should be de-identified immediately (such as where it is being used for analytics or research purposes, which does not require individuals to be personally identifiable).

- Personal information is de-identified 'if the information is no longer about an identifiable individual or an individual who is reasonably identifiable'.
- De-identification involves removing or altering information that identifies an individual or is reasonably likely to do so.
- De-identification includes two steps:



- removing personal identifiers, such as an individual's name, address, date of birth or other identifying information, and
- removing or altering other information that may allow an individual to be identified, for example, because of a rare characteristic of the individual, or a combination of unique or remarkable characteristics that enable identification.
- De-identification may not altogether remove the risk that an individual can be re-identified. There may, for example, be a possibility that another dataset or other information could be matched with the de-identified information. The risk of re-identification must be actively assessed and managed to mitigate this risk.

3. Key Documents

- *Privacy Act 1988 (Cth)*
- *P004 – Privacy Policy*
- *P010 – Finance Policy*

APPROVAL AND REVIEW DETAILS

Approval and Review	Details
Approval Authority	ACSEP Board of Directors
Advisor or Advisory Committee to Approval Authority	ACSEP CEO
Administrator	ACSEP Programs, Policies and Systems Administrator
Next Review Date	April 2027
Approval and Amendment History	
Original Approval Authority	ACSEP CEO
Effective Date	13/07/2016
Amendment Authority and Date	V3 - 14/4/25 – ACSEP Board
Notes	V2 – August 2024 – ACSEP Board V3 – Revised by Russell Kennedy Lawyers