

Guide to best privacy practices for
sporting organisations

Australian Sports Commission

Developed in consultation with Mallesons Stephen Jacques Solicitors

February 2002

Guide to best privacy practices for sporting organisations

1. Introduction

This guide is intended to assist sporting organisations with the new privacy requirements applying to private-sector bodies under the *Privacy Act 1988*. Those obligations commenced on 21 December 2001, although some organisations covered by the new requirements will have an extra year in which to comply.

Overview of the new requirements

The Act protects the handling of personal information. Organisations covered by the Act will have to comply either with the National Privacy Principles (NPPs) or a privacy code approved by the Privacy Commissioner. In considering a privacy code proposed by an organisation or industry, the Privacy Commissioner will want to see at least the equivalents of the NPPs included.

In brief, the NPPs require organisations to:

- take reasonable steps to make individuals aware that it is collecting personal information about them, what the information will be used for and to whom it may be disclosed
- keep personal information secure, accurate, complete and up-to-date
- provide individuals with access to their information on request, and to correct that information if it is inaccurate, incomplete or out-of-date
- allow individuals to remain anonymous where lawful and practicable to do so
- not transfer personal information overseas unless certain requirements are met.

The NPPs are outlined in more detail in Part 4 of this guide (page 8). A guide to compliance and best privacy practice is in Part 5 (page 10).

Contents of this guide

The guide includes sections on:

- Does the Privacy Act apply to my organisation? (page 3)
- When does the new regime start? (page 3)
- What is 'personal information'? (page 7)
- The National Privacy Principles (page 8)

- What should I do if the Act applies to my organisation? (page 10)
- What should I include in my privacy policy? (page 16)

The intention is to provide an overview of the new regime, and answer the questions that most commonly arise for sporting bodies. However, privacy is a complex area and you may need to seek expert advice in some cases.

Regardless of whether the Act applies to your organisation, the principles established by the Act provide a useful guide as to how your members' information can be protected. Sporting organisations may wish to review their current practices for collecting, storing, using and disclosing personal information about their members in light of the new regime.

Further information is available on the Privacy Commissioner's website at 'www.privacy.gov.au'.

Guide to best privacy practices for sporting organisations

2. Does the Privacy Act apply to my organisation?

The new regime will apply to:

- all private sector sporting organisations with an annual turnover of more than \$3 million; and
- some sporting organisations with a turnover of less than \$3 million.

If your turnover is less than \$3 million, the regime will only apply to you if you are:

- a related body corporate of a larger organisation; or
- a dealer in personal information; or
- involved in providing services to the Commonwealth; or
- a health service provider.

These four categories are explained in more detail below. Many sporting organisations will not come within any of these categories, but you should check to see whether your organisation does.

Parts 5 and 6 of this guide explain what you need to do if you are covered by the Act.

When does the new regime start?

The new regime starts on 21 December 2001 for:

- organisations with an annual turnover of more than \$3 million; and
- health service providers (regardless of what their turnover is).

For all other organisations covered by the regime, it starts on 21 December 2002.

Related body corporates

A private sector body will be covered by the new regime if it has a 'related body corporate' with an annual turnover of more than \$3 million.

This is aimed at the situation where a large company has a small subsidiary. Both the large company and the small subsidiary have to comply with the Act. This situation may not apply to many sporting bodies, however.

You are not a related body corporate of a bigger organisation just because you are a member of that organisation (eg a local club that is a member of a state body, or a state body that is a member of an NSO). They would need to own or control more than 50% of your organisation for you to be a related body corporate.

Dealers in personal information

Your organisation may be a 'dealer in personal information' if you:

- disclose personal information to anyone else for a benefit, service or advantage; or
- provide a benefit, service or advantage to collect personal information from anyone else.

For example, providing personal information about your members to a state body or NSO could make you a dealer in personal information if you receive services from the state body or NSO in return (eg coaching, insurance or access to facilities).

However, you will not be a dealer in personal information if you provide that information:

- with the consent of the persons whose information is being provided (eg your members); or
- as authorised by particular legislation.

Most sporting bodies will not be authorised by legislation to pass personal information on to other organisations, but it would be relatively easy for you to get the consent of your members to provide information about them to the relevant state body and NSO, and you would then not be a dealer in personal information. The simplest way to obtain member consent may be to include a statement on your membership renewal form.

Involved in providing services to the Commonwealth

Your organisation will be subject to the new regime if you:

- have a contract with the Commonwealth or a Commonwealth agency to provide them with services; or
- are a subcontractor to another organisation providing services to the Commonwealth or a Commonwealth agency.

Examples of services provided to the Commonwealth or an agency under contract might include providing advice (eg about sporting issues), preparing a report (eg on grass-roots sporting membership), providing sporting services (eg coaching) or providing facilities (eg a sporting complex or function facilities).

If you receive a grant from the Commonwealth or an agency, for example to assist in preparing for the Olympic Games, that does not mean you are providing a service, even if you have to report to the Commonwealth on the way the funds were spent, or about the activities you undertook.

Other issues

If the new privacy regime applies to you because you are providing services to the Commonwealth or to an agency, that regime will only apply to the services provided under the contract, not to any other activities of your organisation.

You may also be required by the Commonwealth or an agency as part of your contract to comply with the public sector privacy regime. If entering into a contract to provide services to the Commonwealth or an agency, you should ask your lawyer for advice about this.

Health service provider

Your organisation will be a 'health service provider' if you:

- provide a health service to individuals; and
- hold any health information about them (except information about your own employees).

You will only be a health service provider if you do both these things, so if you only do one or the other, this section will not apply to you.

Even if you are not a health service provider, it would be good practice to review the terms of your contracts with other health service providers (eg physios) to ensure they seek permission from the athletes being treated for the appropriate health information to be passed on to you.

Do you hold health information?

If you do not hold any health information, you will not be a health service provider.

It does not matter if you provide some health services (eg physiotherapy or massage) - that does not make you a health service provider if you are not holding health information about people.

Health information is defined as:

'Health information includes:

- *information or an opinion about:*
 - *the health or disability (at any time) of an individual;*
 - *their expressed wishes about the future provision of health services to them; or*
 - *a health service provided, or to be provided, to an individual;*
- *other personal information collected to provide, or in providing, a health service; or*
- *other personal information about an individual collected in connection with the donation, or intended donation, by them of their body parts, organs or body substances.'*

If in doubt about this definition, seek advice.

Do you provide any health services?

If you do not provide any health services, you will not be a health service provider.

It does not matter if you keep information about people's health (eg asthma, allergies, disabilities) for club purposes, such as eligibility for events or for your general duty of care - that does not make you a health service provider if you are not providing any health services.

'A health service means:

- *an activity performed in relation to an individual that is intended or claimed by the person performing it:*
 - *to assess, record, maintain or improve the individual's health; or*
 - *to diagnose the individual's illness or disability; or*
 - *to treat the individual's illness or disability (whether suspected or real); or*
- *dispensing on prescription of drugs/ medicines by a pharmacist.'*

If in doubt about this definition, seek advice.

Guide to best privacy practices for sporting organisations

3. What is 'personal information'?

Personal information is defined in the Act as:

'information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion'.

Guide to best privacy practices for sporting organisations

4. The National Privacy Principles

A brief overview of the 10 National Privacy Principles (**NPPs**) is set out below. The full text of the NPPs is available on the Privacy Commissioner's website at www.privacy.gov.au.

1. Collection

Ensure that the collection of personal information is necessary, that you use lawful and fair means and (where reasonable and practicable) that it is collected directly from the individual.

Ensure that the individual is told your organisation's name, the purpose for collection, the types of organisations to which the information is usually disclosed and that the individual can access the information.

2. Use and disclosure

Use and disclose personal information only for the purpose that it was collected for, or for a related (or directly related if the information is sensitive) secondary purpose. Exceptions cover specified direct marketing, law enforcement and public safety purposes.

Obtain consents for the uses or disclosures of personal information for other unrelated purposes.

3. Accuracy

Ensure that the personal information you collect, use or disclose is accurate, complete and up-to-date.

4. Security

Ensure that all personal information stored is safe from misuse, unauthorised access or disclosure. Where reasonable, destroy or permanently de-identify personal information if it is no longer needed.

5. Privacy Policy

Have a freely available policy summarising your personal information handling practices. Be able to provide more detailed information about those practices upon request.

6. Access and correction

Provide individuals with access to the personal information that you hold about them upon request (some exceptions apply). Give them a reasonable opportunity to correct that information.

7. Identifiers

Do not use or adopt identifiers assigned by Commonwealth government agencies to individuals, eg Medicare numbers.

8. Anonymity

Allow individuals the right to remain anonymous when it is lawful and practicable to do so.

9. Overseas Transfer

Ensure that personal information is transferred overseas only to a country with an equivalent privacy regime, or with the individual's consent, or if the transfer benefits the individual.

10. Sensitive information

Do not collect sensitive information without a person's consent (some exceptions apply) eg information about an individual's health, racial origin, political opinions or affiliations, religious or philosophical beliefs, professional/trade union membership, sexual preferences or criminal record.

Guide to best privacy practices for sporting organisations

5. What should I do if the Act applies to my organisation?

The table set out below provides an overview of the new privacy regime and a guide to best privacy practices. The 10 National Privacy Principles (**NPPs**) are referred to throughout the table.

The table covers the following areas:

- 1 establishment of a compliance regime;
- 2 what to do for general ongoing compliance;
- 3 what to do when collecting personal information;
- 4 how to deal with a request from a person for access to their information;
- 5 overseas transfer of personal information;
- 6 rules for use and disclosure of personal information.

Guide to best privacy practices for sporting organisations

Requirement	Suggested action
<p>1 Establishment of compliance regime</p>	<ul style="list-style-type: none"> • Appoint a privacy officer (eg combine this task with your club registrar) • Develop a privacy policy (for details see Part 6 of this guide on page 16) [NPP 5.1] • Have a secure system for storing personal information (eg stored on a computer with access limited to specified club officers) [NPP 4.1] • Train staff in privacy requirements (this table explains the key things they need to know) • Your system must not list or index information by government identifiers except by ABNs (eg tax file numbers, medicare numbers are prohibited) [NPP 7] <p><i>General rule: treat all personal information held by your organisation as if the new regime applies to it, even if it was collected before the new regime commenced</i></p>
<p>2 General ongoing compliance</p>	<ul style="list-style-type: none"> • Keep personal information accurate, complete and up-to-date [NPP 3] This could be done by including a section in your membership and renewal forms asking members to let you know if their details have changed In addition, if the consequences of use of the information could be severe for the person (eg disciplinary proceedings), it may also be prudent to check whether the information is accurate, complete and up-to-date <u>before use</u> • Review system security [NPP 4.1] and staff training periodically (it is suggested that a review once a year would be reasonable, eg as part of the handover to the incoming committee) • Destroy information or de-identify when no longer used or needed [NPP 4.2] (again, it is suggested that an annual review would be reasonable for this purpose)

Requirement	Suggested action
<p>3 At time of collection</p>	<ul style="list-style-type: none"> • Only collect personal information that is <i>necessary</i> [NPP 1.1] (eg name, address and phone numbers are clearly necessary information to hold about members) • Only use <i>lawful and fair means</i>, and do not act in an <i>unreasonably intrusive way</i> [NPP 1.2] • Where lawful and practicable, give individuals the option of remaining <i>anonymous</i> [NPP 8] Obviously you will need names for people joining or renewing their membership, but information collected from other activities (eg fundraising) could be anonymous if people wish • Where reasonable and practicable, collect information <i>directly</i> from the individual [NPP 1.4] • Take reasonable steps to inform the individual of [NPPs 1.3 and 1.5]: <ul style="list-style-type: none"> ➤ your organisation’s contact details; ➤ all proposed uses and disclosures of the personal information (eg will be passed on to the state association for team/grade registration and insurance and the national association for insurance and national communications); ➤ how to access the information (eg contact the club registrar if you wish to change or confirm your details); ➤ any law that requires the information to be collected; and ➤ the consequences if any part of the information is not provided (eg without your name and address details, we will be unable to register you and you cannot play) <p>UNLESS providing this information would seriously threaten life or health (this exemption only applies where collection is through a third party, not where it is collected directly)</p> <p>You might want to have a standard blurb with these details that could be provided when the information is collected, eg:</p> <p><i>‘Your privacy is respected by us. The information you provide on this form may be used to [] and may be provided to [].</i></p> <p><i>If you have any privacy concerns or would like to verify information we hold about you, please contact our privacy officer on [].</i></p>

Requirement	Suggested action
	<p><i>If you do not provide the information requested on this form, we may not be able to register you as a member.'</i></p>
	<ul style="list-style-type: none"> • Obtain <i>express consent</i> to collection of any 'sensitive information' [NPP 10] <i>Sensitive information</i> is information or an opinion about a person's health, race/ethnicity, political opinions, membership of a political association, religious/ philosophical beliefs or affiliations, professional/ trade association membership, trade union membership, sexual preferences/ practices or criminal record, eg you might need to collect information about people's health if going on an interstate trip. In the event of an accident, the information would be given to appropriate medical professionals for treatment. This information would be destroyed after the trip. Exemptions apply - eg collection required by law, certain non-profit situations, health emergency, legal claims - seek advice where required. • Where practicable, obtain <i>express consent</i> to all proposed uses and disclosures of information [See point 6 of this table for permitted use and disclosure] • <i>NOTE: the obligations in this section 3 only apply to information collected on or after commencement¹</i>
4 Requests for access	<ul style="list-style-type: none"> • Provide individuals with access to their personal information on request (see the example in section 3 of this table above) [NPP 6] <i>Exemptions apply - eg health emergency situations or protecting others' privacy, current negotiations, law enforcement/ investigation, certain commercially sensitive processes - seek advice where required</i> • Take reasonable steps to correct an individual's information so that it is accurate, complete and up-to-date [NPP6] • Make your privacy policy available to anyone who asks for it (eg put it on your club website) [NPP5.1] • Let individuals know, on request, what sort of information is held about them, for what purposes and how you

¹ The commencement date depends on your organisation. See page 2.

Requirement	Suggested action
	<p>collect, hold, use and disclose that information (in general terms) [NPP 5.2]</p> <p>You could have a standard blurb that the club secretary could provide if people ask, and on the club website</p> <p><i>NOTE: the obligations to provide access and correction only apply to personal information collected <u>before commencement</u> if:</i></p> <ul style="list-style-type: none"> ➤ <i>the information is used or disclosed by your organisation on or after commencement; and</i> ➤ <i>providing access and correction rights will not cause you an unreasonable administrative burden or expense</i>
<p>5 Overseas transfer of information</p>	<ul style="list-style-type: none"> • You may transfer personal information overseas if the transfer is for the individual’s benefit (and it is not practical to get their consent), or if the individual has consented to the transfer [NPP 9] <p>For example, for international competitions you may need to provide members’ names and addresses, and it would be preferable to provide this information on announcing the team, once the team members had agreed for the information to be passed on to the international body</p> <ul style="list-style-type: none"> • Otherwise, ensure that the transferred information will be protected in a manner consistent with the National Privacy Principles - seek advice on detailed requirements of NPP 9
<p>6 Use and disclosure</p>	<p><i>Note: the obligations in this section 6 only apply to information collected <u>on or after commencement</u>²</i></p> <p>Personal information:</p> <ul style="list-style-type: none"> • Where possible, obtain <i>written consent</i> to all uses and disclosures <p>The easiest time to do this may be when you are collecting the information from them, eg when a new member joins your club, or when existing members renew their membership</p> <ul style="list-style-type: none"> • Consent is not required (but is recommended) if the use or disclosure is <i>related to</i> the primary purpose of collection, and is for a purpose which the individual would <i>reasonably expect</i> [NPP 2] <p><i>eg where a hockey association has collected members’ details for registration purposes, the following would be related purposes:</i></p>

² The commencement date depends on your organisation. See page 2.

Requirement	Suggested action
	<ul style="list-style-type: none"> - <i>sending members the club policy and renewal papers</i>
	<ul style="list-style-type: none"> - <i>sending members information about pending district, state and national hockey tournaments or new member services</i> <p><i>This would <u>not</u> allow:</i></p> <ul style="list-style-type: none"> - <i>sending members' addresses to a marketing organisation</i> - <i>sending members advertising material from sponsors or anyone else</i> <p><i>The club <u>can</u> send advertising material to members if it is easy (and free) for them to 'opt out' of receiving it, eg:</i></p> <ul style="list-style-type: none"> - <i>tick a box on the membership or renewal form;</i> - <i>tick a box in a cover letter sent with the advertising material (and include a reply paid envelope); or</i> - <i>call a toll free phone line.</i> <p>In some other cases, consent is not required - eg certain health emergencies, as required by law (eg court subpoena or police checks for people working with children required under State law), law enforcement/ investigation (eg police warrant), and public health research situations - seek advice where required</p> <p>Sensitive information:</p> <ul style="list-style-type: none"> • Obtain <i>written consent</i> to all uses and disclosures <ul style="list-style-type: none"> <i>Sensitive information is information or an opinion about a person's health, race/ethnicity, political opinions, membership of a political association, religious/ philosophical beliefs or affiliations, professional/ trade association membership, trade union membership, sexual preferences/ practices or criminal record</i> <p>Again, the easiest time to obtain consent may be when a member joins or renews their membership</p> • Consent is not required (but is recommended) if the use or disclosure is <i>directly related to</i> the primary purpose of collection, and is for a purpose which the individual would <i>reasonably expect</i>. This is a very strict test, and covers little more than the original purpose of collection [NPP 2] <ul style="list-style-type: none"> <i>For example, informing a member of a new treatment for an injury or medical condition they have, or internal administrative purposes</i> • In some other cases, consent is not required - eg certain health emergencies, law enforcement/ investigation,

Requirement	Suggested action
	public health research situations - seek advice where required

Guide to best privacy practices for sporting organisations

6. What should I include in my privacy policy?

Guidelines released by the Privacy Commissioner indicate that a privacy policy should be a short and clearly expressed statement that covers:

- whether your organisation is bound by the National Privacy Principles or a code approved by the Commissioner (including a reference to the code);
- any exemptions under the Privacy Act that apply to the information your organisation holds or to any of its acts or practices;
- the kind of personal information your organisation holds, eg contact personal information details, health information, financial information, any 'sensitive information';
- the main purposes for which your organisation uses that information;
- how your organisation keeps the information secure and protects it from misuse, loss and unauthorised disclosure;
- whether your organisation contracts out services, or is itself a contractor to the Commonwealth or a State government;
- how an individual can complain about possible breaches of privacy including the contact number of your organisation's privacy representative;
- your organisation's full contact details; and
- how your organisation will handle requests for access to personal information.

