

The National Privacy Principles and the Internet



How Australia's
new privacy laws
affect your
organisation on the
Internet

A special report from
**First Step
Communications**

www.firststep.com.au

Copyright

This report is copyright. Apart from any fair dealing for the purpose of private study, research, criticism or review, as permitted under the Copyright Act, no part may be reproduced by any process without written permission from the publisher.

Liability disclaimer

The material contained in this report is general and is not intended as advice on any particular matter. First Step Communications and the author expressly disclaim all and any liability to any persons whatsoever in respect of anything done by any such person in reliance, whether in whole or in part, on this report. Please take appropriate legal advice before acting on any information in this report.

About This Report

Since 21st December 2001, many Australian businesses have been obliged to operate under new privacy provisions, known as the National Privacy Principles (or NPPs), in the Privacy Act.

This report describes how the changes affect your organisation's use of the Internet – in particular, when sending e-mail and operating your Web site.

The new laws apply broadly to all areas of your business, and this report only covers Internet-related aspects. Please refer to other material for information about the wider application of the new privacy laws.

Even within the narrower scope of Internet-related activities, we only cover the more common privacy issues here. Your organisation might be affected in other ways, so again we urge you to seek information elsewhere as well.

Health services

Health service providers deal with very personal information, so the Act imposes more restrictions on them. As we have yet to work with clients in the health services area, we do not cover these requirements here.

Netiquette

In addition to the legal requirements, Internet users have created a set of informal rules of etiquette, known as "netiquette", for acting responsibly on the Internet. These rules often go beyond the legal requirements of the new privacy provisions, so we consider some of them as well.

Frequently Asked Questions

Do the new laws apply to me?

Broadly, the two main groups affected by the new laws are health service providers and organisations with an annual turnover exceeding \$3 million. This includes non-profit organisations.

If your organisation falls outside this range, it's *generally* exempt from the new laws. However, there are some exceptions, such as:

- Organisations that sell personal information (such as mailing list companies)
- Commonwealth government contractors
- Organisations that *choose* to "opt in" to the new provisions (say, to increase consumer confidence)

If they don't apply to me, should I care?

If you don't fall into any of the categories above, it's not *compulsory* for you to follow the privacy provisions. However, the privacy provisions are excellent guidelines to good business practice. We recommend that you follow them anyway, even if you don't formally opt in to them.

What is personal information?

Broadly, it refers to any information about an individual that can be used to identify that individual.

This includes information you've collected from the individual, from third parties, and from internal notes recorded about that individual within your organisation.

Should I get independent legal advice?

The new privacy provisions are *laws*, so yes, we recommend that you seek legal advice about applying them to your organisation.

Much of the information in this report is based on information provided by the Office of the Privacy Commissioner. Even the Office acknowledges that it's only providing general explanations and tips, not legally binding advice. This is what it says on its Web site:

“Information sheets are based on the Office’s understanding of how the Privacy Act works. They provide explanations of some of the terms used in the NPPs and good practice or compliance tips. They are intended to help organisations apply the NPPs in ordinary circumstances. Organisations may need to seek separate legal advice on the application of the Privacy Act to their particular situation.”

Overview of the NPPs

This page presents a brief summary of the ten National Privacy Principles.

1. **Collection:** Only collect personal information that's necessary; collect it by lawful, non-intrusive means; collect it from the person directly.
2. **Use and disclosure:** Only use the information as originally intended; get the person's consent before using it for other purposes.
3. **Data quality:** Take reasonable steps to keep the information accurate, complete and current.
4. **Data security:** Keep the information safe; destroy it if it's no longer required.
5. **Openness:** Publish a privacy policy.
6. **Access and correction:** If asked, tell people what information you hold about them; give them a process to correct it if required.
7. **Identifiers:** Use your own means of identifying a person. Don't use government identifiers, such as a Medicare number.
8. **Anonymity:** If practical, allow people the option of remaining anonymous when dealing with you.
9. **Transborder data flows:** Share the information with non-Australian companies only if they have similar privacy provisions.
10. **Sensitive information:** Don't collect sensitive information without consent.

The next ten sections of the report deal with each of the NPPs in turn, and how they relate to the Internet.

NPP1 – Collection

NPP1 describes the process of collecting personal information. This might apply to you in a number of ways on the Internet, including:

- Incoming e-mail
- Forms that visitors complete on your Web site
- Cookies
- Web “bugs” embedded in outgoing e-mail
- User registration at your Web site
- Subscription to an e-mail newsletter

NPP1 requires you to:

- Only collect personal information if it’s necessary.
- Collect it by lawful, fair and non-intrusive means.
- Tell people about the information you are collecting.
- Collect it directly from the individual concerned.

Look at all the places where you collect information, and consider whether you meet these requirements. Some things to consider:

- Do you collect information over and above what’s *necessary*?
- If so, is this information optional? Good netiquette says that you should only make the necessary information compulsory, and leave the rest optional.
- Is there a legitimate reason for asking for this information? If so, do you tell people why you’re collecting it?

Your Web site’s privacy policy can deal with some of these issues, and we deal with this later.

Collecting information from third parties

Although it seems like a good idea to ask site visitors to “register their friends” for a service on your site (such as an e-mail newsletter), it’s better to ask them to refer their friends to your site, and leave it to the friends to decide whether to register.

If you *do* ask a site visitor for personal information about somebody else, notify that other person as soon as it’s practical.

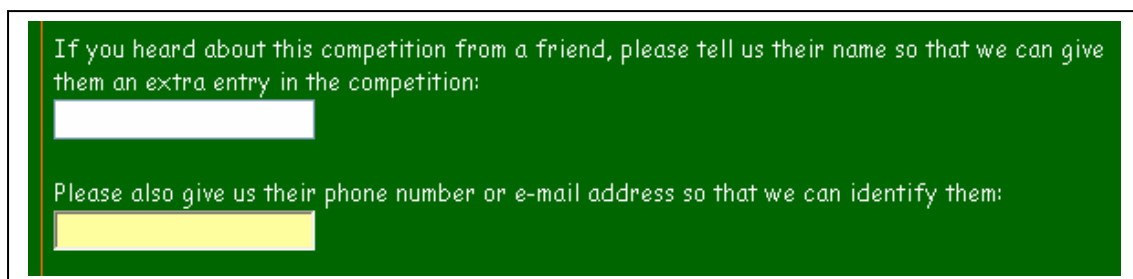
Examples

Here is an example from one of our clients, Max Hitchins, on his site www.themelbournecup.com.au.

Max runs a free competition for site visitors. When they enter the competition, he would like them to refer the site to a friend. If the friend also enters the competition, the person who referred them gets another entry, thereby increasing their chances.

The *wrong* way to do this is to ask the first person for their friend's e-mail address and enter them in the competition directly, because that would be happening without the friend's permission.

The better solution is to ask the first person to recommend the site to their friend, and when the friend enters the competition, the site asks them for the person who referred them:



If you heard about this competition from a friend, please tell us their name so that we can give them an extra entry in the competition:

Please also give us their phone number or e-mail address so that we can identify them:

Another example is from our own site www.firststep.com.au. When people enrol in our free newsletter, we ask them whether they heard about the site from an existing subscriber, so we can send that person a gift:



First Name:

Last Name:

E-Mail Address:

How did you hear about this newsletter?

Details (if applicable):

Again, it would be slightly easier to simply ask the existing subscriber to add their friends to our mailing list, but some of the "friends" would definitely – and rightly – object.

NPP2 – Use and disclosure

This is the principle that will probably have the greatest impact on your organisation. “Use” refers to you using personal information in your organisation, and “disclosure” refers to you telling others about it (except for the individual themselves – this is called “access”, and is covered by NPP6).

Primary purpose

In general, you can only use information for *the primary purpose* for which it was collected. The primary purpose is usually clear – for example, buying products from your Web site, signing up to an e-mail newsletter, or completing a customer feedback form.

If you have additional purposes in mind, *say so on your Web site* when you collect the information.

This clause has some exceptions, and some are directly related to Internet use.

Related secondary purpose

You can use information for *a secondary purpose*, provided it’s related to the primary purpose and the individual would reasonably expect you to use it for this secondary purpose.

The Privacy Commissioner describes “reasonably expect” as what an individual with no special knowledge of the industry or activity involved would expect.

For example, if a customer buys a product from you, and you send them marketing information about a related product or an upgrade, that would probably be considered to be a related secondary purpose. On the other hand, if you exchange business cards with somebody at a networking function, and you add them to your mailing list without their permission, that would probably *not* be considered a related secondary purpose.

Again, if in doubt, *tell your site visitors* about your intended uses for collecting the information, so that they can make an informed choice about providing it.

Opt-in and opt-out

Of course, if people consent to you using or disclosing their personal information, you can do so.

There are two ways of obtaining consent:

- “Opt in”, where users take some action to indicate their consent.
- “Opt out”, where users take some action to **deny** consent.

For example, consider a Web site with an on-line order form. When customers place an order, it's common to ask them whether they would like to receive future marketing e-mail from you. The opt-in approach is to include them on the mailing list only if they say so (for example, by checking a box on a form), while the opt-out approach is to include them *unless* they say otherwise.

Opt-in is more “user friendly” because privacy is assumed unless consent is explicitly given. Good netiquette says that you should offer opt-in rather than opt-out.

The law, on the other hand, allows you to use opt-out, provided you present this option clearly and make it easy for users to choose it.

Our Recommendation

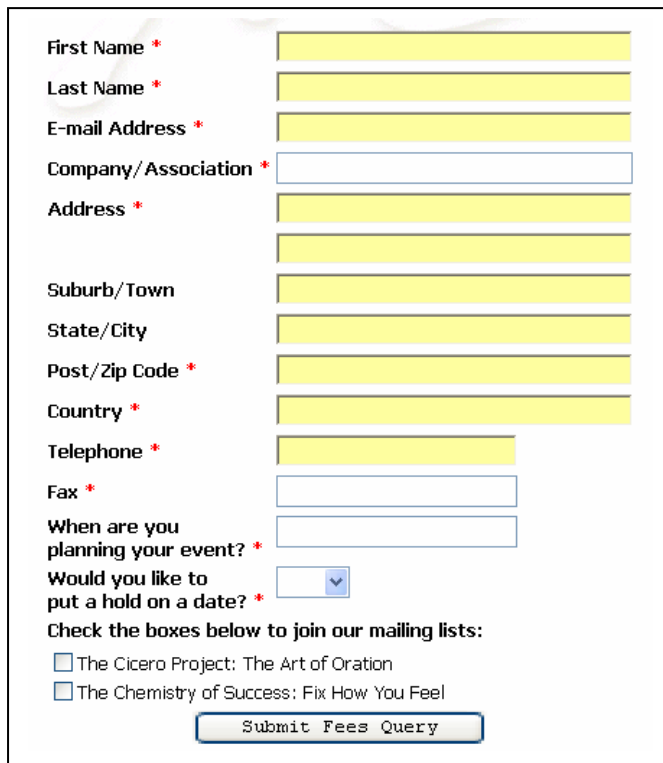
We recommend that you practise good netiquette and choose the more conservative opt-in approach.

The trouble with opt-out is that, even though it's allowed by law, some Internet users get very upset by it. They can retaliate by sending you nasty e-mail, reporting you as a spammer to your Internet Service Provider, report you to e-mail blocking services, or take revenge by flooding your in-box with junk mail. Sometimes it takes just one complaint to have your e-mail blocked or your account closed. Even though you can appeal against this process, it can waste your time and cost you business.

If, despite our advice, you do decide to use opt-out, make every effort to make this option easy to understand and use.

Examples

Here's an example from one of our clients, Matt Church, who uses the (recommended) opt-in approach on his Web site www.mattchurch.com:



First Name *

Last Name *

E-mail Address *

Company/Association *

Address *

Suburb/Town

State/City

Post/Zip Code *

Country *

Telephone *

Fax *

When are you planning your event? *

Would you like to put a hold on a date? *

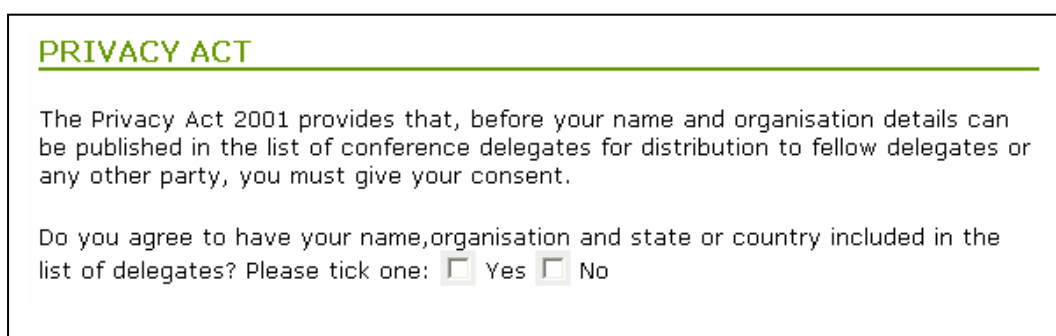
Check the boxes below to join our mailing lists:

The Cicero Project: The Art of Oration

The Chemistry of Success: Fix How You Feel

This is an enquiry form on Matt's site, with the option at the end of the form for the Web site visitor to subscribe ("opt in") to his two mailing lists. If the two boxes were already checked, and the site visitor had to un-check them, that would be "opt out", which is not recommended.

Another example is from another client, Congress West, at www.congresswest.com.au, a professional conference organiser in Western Australia. Congress West publishes lists of conference delegates to sponsors and other third parties, so it requires each delegate's explicit permission to do so. When a delegate registers for the conference, they are asked this question:



PRIVACY ACT

The Privacy Act 2001 provides that, before your name and organisation details can be published in the list of conference delegates for distribution to fellow delegates or any other party, you must give your consent.

Do you agree to have your name, organisation and state or country included in the list of delegates? Please tick one: Yes No

The registration form is programmed so that this question is compulsory, so that there is no doubt at all about the delegate's intention.

Direct Marketing

The privacy provisions allow you to use personal information for direct marketing, provided it's impractical to gain consent before use, people can request to be removed from future direct marketing, and each direct marketing piece tells them about this option to opt out.

Getting consent

The above conditions apply to direct marketing in general. What about marketing by e-mail specifically?

The Privacy Commissioner has already taken a stand on this issue, making the point that it's usually *not impractical to seek consent from individuals by e-mail*, and going on to say that

“generally an organisation could not rely on [this clause] for techniques such as email marketing or SMS marketing.”

In other words, the law requires you to obtain consent before sending marketing material by e-mail.

The Privacy Commissioner also warns that

“It is unlikely that consent to receive marketing material on-line could be implied from a failure to object to it.”

In other words, just because you send marketing e-mail to people and they don't object, that doesn't imply that you have their consent.

There's a good reason for this. Many Internet users are suspicious of promises along the lines of “To stop receiving this e-mail, reply and we'll remove you immediately from the mailing list” because unscrupulous junk mailers commonly use this trick to determine who reads their e-mail (and hence is a target for even more junk mail). So even if you attempt to do the right thing, your recipients have no way of knowing that you're honest.

Good netiquette

If you follow the reasoning above, you can infer that the law *does* allow you to e-mail people first, asking them for permission to send them on-line marketing material.

However, many Internet users consider even this initial e-mail as a breach of netiquette. We recommend that you *only* send e-mail to people who have specifically given you their e-mail address and could reasonably expect to receive e-mail from you.

You may have received marketing e-mail that uses some of these techniques:

- A marketing message sent directly without asking for permission, and without any reference to opt out of receiving future message.
- An initial enquiry asking whether you are interested in receiving marketing e-mail, with an option to opt out of receiving future messages (e.g. something along the lines of "Reply to this e-mail to unsubscribe from our mailing list").
- An initial enquiry message, telling you how to subscribe to receiving marketing material.

The first is clearly a breach of the law. The second is probably also a breach, because failure to object does not imply consent, as noted above. The last option is allowed by the law, however it's frowned upon as poor netiquette.

Privacy requirements cross companies

Following the dot-com crash in the United States, some Internet companies attempted to raise money by selling their databases to other companies. This caused a justifiable uproar among Internet users, and even prompted Amazon.com to update its privacy policy to protect itself from a similar result.

The new privacy provisions prevent this sort of use without consent. They say that the primary purpose for which the information was collected remains the same, even if another company is now using it. For example, if you sell your mailing list to another organisation, they are bound by the same "primary purpose" restrictions as you are.

Of course, this requirement also applies the other way around – if you are *receiving* personal information from another organisation. In particular, be careful about buying lists of e-mail addresses. It's often difficult to verify that everybody on the list has given their consent to be on the list, much less to receive *your* marketing material.

NPP3 – Data quality

NPP3 requires you to keep information accurate, complete and up-to-date.

On the Internet, this will most likely affect you with e-mail addresses, because people change them frequently. So make every effort to keep your list of e-mail addresses current. This is not only required by law; it's also part of being a good Internet citizen because it reduces the load on the Internet caused by sending e-mail to wrong or non-existent addresses.

NPP4 – Data security

You are required to keep the information that you collect safe and secure.

Be careful about how you store any personal information that you collect. Evaluate the risks and consider using an experienced IT security consultant to advise you in this area.

Individual access

If your Web site allows people to register on-line and store personal information, take reasonable steps to ensure that only the individual themselves can access their personal information.

This usually means creating a password for each user (Either users choose a password, or your system generates a password for them).

For example, people who sign up for our free G'day Australia service (www.firststep.com.au/gday) choose a password when they sign up:



The screenshot shows the registration page for G'day Australia. At the top, there is a logo with a sun and a green arrow pointing to the text 'G'day Australia'. Below the logo, it says 'From First Step Communications'. The main heading is 'New Member'. The text below says 'To become a member, fill in the form below and press the "Sign Up!" button.' The section 'Your Password' asks the user to choose a password that will be known only to them and to type it twice for verification. It also advises to choose a different password from other services and not to use a bank card's PIN. The registration form has four fields: 'Your Name' (a single text box), 'Password' (two text boxes for entering and confirming the password), 'State' (a dropdown menu currently set to 'Outside Australia'), and 'How did you hear about G'day Australia?' (a text box).

Your Name	<input type="text"/>
Password	<input type="text"/> <input type="text"/>
State	Outside Australia <input type="button" value="v"/>
How did you hear about G'day Australia?	<input type="text"/>

Be careful about asking people to identify themselves just by name and/or e-mail address. This is not private enough, and it's too easy for imposters to guess them.

Computer networks

If you hold personal information on any computer or network connected to the Internet (even if it's only connected temporarily via a dial-up modem), this opens up the possibility of outsiders "hacking in" to your computer.

At a minimum, install a firewall between your computer network and the Internet.

If you're one of the many Internet users moving to a broadband connection (cable, ADSL or satellite), be especially careful because your computer is now connected to the Internet more often, so this increases the risk of hackers.

For more information about PC security, read "**The Common Sense Guide to PC Security**" at www.firststep.com.au/pc-security.html.

Web servers

If your Web site stores personal information in an on-line database on your Web server, it's permanently connected to the Internet, so hackers have a greater "window of opportunity" to gain access.

Most reputable Web site hosts work diligently to maintain the security of their Web servers, so talk to your site host to ensure that they have taken this into account.

In particular, if you share the Web server with other users (this is common), ensure that your database is accessible only to you. We have come across Web site hosts in the past where this is not the case, so any hacker can easily access personal information on your site simply by signing up for an account with the same Web host.

Credit card information

Be especially careful if you store credit card information on your Web server. Although most Internet users expect you to use a secure server to protect their credit card details from hackers as the information goes from their browser to your Web site, the greater potential risk is storing them on your server.

For greatest protection, don't store credit card information at all on the Web server. Use it for one transaction only, then let it evaporate into cyberspace.

If this is impractical (if, for example, you require credit card details for monthly payments), we strongly recommend that you talk to a security consultant.

Accidental disclosure

It's your responsibility to keep personal information secure. Even if you disclose information accidentally, that doesn't necessarily protect you from being prosecuted under the Act.

Here are some examples of real-life privacy breaches on the Internet. We recommend that you read them and put procedures in place in *your* business to prevent similar occurrences.

Examples

From time to time, you will read stories of users logging in to a private account on a Web site, only to find that the site has given them access to another user's account. This has happened with e-mail providers, government Web sites and even banks. This usually happens after a software change, so test your software upgrades carefully.

Another form of inadvertent disclosure happens in e-mail, when everybody on a mailing list sees everybody else's e-mail address. This usually happens when the list owner sends a newsletter using their standard e-mail program (such as Eudora, Outlook or Netscape Messenger). If you send your newsletter this way, use Bcc instead of Cc when sending the e-mail.

An even simpler form of e-mail disclosure happens when somebody sends an e-mail message to the wrong address. I recently received a misdirected e-mail message from the office of a large franchise company, showing the performance of all their franchisees around Australia! Take care when addressing e-mail, because even one mistyped letter can mean disaster.

Another type of accidental disclosure occurs when somebody puts a private document somewhere on a publicly-accessible Web site. Even if the only link to that document is in an obscure, hard-to-find place, search engines like Google are likely to find that link and add it to their database, thus making the "private" document readable by anybody. Security experts have demonstrated this flaw by successfully finding credit card numbers, medical records, student grades, and even lists of suspected terrorists – all by doing public searches using Google.

Another example: The on-line ticketing agency Ticketmaster7 has been investigated by the Privacy Commissioner for breaches to the Privacy Act. It was discovered that site visitors could get access to other people's personal information simply by altering the Web address slightly when making a booking. Ticketmaster7 escaped punishment because they fixed the problem quickly and no customers had complained; however, the next company in that situation might not be so lucky.

Destroy or permanently de-identify old information

If you collect some information only for statistical purposes (for example, asking demographic questions so that you can tell potential advertisers about your typical visitors), “de-identify” it by removing anything that matches that information to an individual.

In general, your Web server logs do not present enough information to identify individuals. However, if you combine this information with information collected in another way (for example, cookies or Web forms), it might be possible to identify individuals and their surfing habits.

NPP5 – Openness

Create a privacy policy and publish it prominently. Place it clearly on your Web site, with a link to it on every page that collects personal information.

The Privacy Act itself doesn’t specify what has to be in a privacy policy, though it does say that a privacy policy is required:

“An organisation must set out in a document clearly expressed policies on its management of personal information. The organisation must make the document available to anyone who asks for it.”

Although the Act is fairly general about your privacy policy, we do have specific suggestions about how to write a privacy policy for your Web site. Read on ...

In your privacy policy, tell people:

- The kind of personal information you hold
- What you do with it
- Whether you disclose it to contractors
- How to get in touch with you
- How people can complain about a breach of privacy
- How you handle requests for personal information

Remember that this isn’t required by the Act; it’s just our recommendation.

Some Web sites and e-mail newsletters just have something short and sweet, like this (from our client Rachel Green’s newsletter www.RachelGreen.com):

Reflections is only sent to those who have requested it. I protect your privacy and never share our mailing list with anyone.

Here's an example from another client, Colin Pearce, at www.ColinPearce.com, who gets the best of both worlds with a brief privacy statement that contains a link to a more detailed privacy policy:

Privacy Note:
In accordance with the Australian Commonwealth Government's National Privacy Principles we are happy to tell you that we won't give your details to anyone without your consent.
For the full story read our [Privacy Policy](#).

You'll find our privacy policy in the Appendix. Feel free to copy this for your own use. However, we don't claim that it will suit your requirements, so we strongly recommend that you seek independent legal advice.

Explain why you are asking for personal information, especially if the reason is not immediately obvious. This is just good business practice, and the more you explain your reasons up front, the easier it is to use that information later.

If you publish an e-mail newsletter, include a link from it to the privacy page of your Web site.

If you operate more than one Web site, make it clear on each Web site who owns it. Either write a specific privacy policy for each site, or provide a link from each site to your main privacy policy.

NPP6 – Access and correction

You are required to give people, on request, access to the information you hold about them. The Privacy Commissioner suggests that 14 days is a reasonable turnaround for straightforward requests, and 30 days for more complex requests.

Verify their identity

It's important to verify that the person requesting the information is in fact who they say they are. Otherwise you are in danger of "disclosing" the information in breach of NPP2.

In particular, be very careful when replying to an e-mail request for information. E-mail is relatively easy to forge, and some scammers can trick you into disclosing other people's personal information.

For example, if you receive e-mail from somebody at MICROSOFT.COM, only an alert person will notice that this is not the same as MICROSOFT.COM (If you still don't see the difference, compare the letter "o" in the names). A scammer could

register the bogus domain name and use it to send requests for personal information.

Frivolous requests

The law allows you to ignore “frivolous or vexatious” requests. However, the Privacy Commissioner points out that:

“Often, a request for access would not be frivolous or vexatious just because it is irritating. Organisations are encouraged to take a narrow approach to this exception.”

Charging a fee

If you’re providing the information on-line (say, by e-mail or by the user viewing a Web page), your costs are likely to be very low, so consider making this access free to the user. You *can* charge for time spent locating the information, collating it and explaining it to the person requesting it.

This clause refers specifically to financial costs. Consider also the technical and practical costs of people getting in touch with you. It’s good business practice to make it easy for people to get in touch with you. Include your contact information (at least a telephone number and e-mail address) on every page of your Web site. If you use on-line feedback forms, ensure they work in a wide range of browsers (For example, some require JavaScript or other advanced technologies that prevent some users from using them).

Update the information on request

You might offer people ways to update their information themselves on-line – for example, changing their e-mail address for subscription to your newsletter, or changing their registration details.

Even if you do allow people to update their information themselves, it’s polite to update it for them if they ask you to do so. For example, if you operate an on-line newsletter, you should tell subscribers how to opt out of future issues. Some subscribers will ignore the instructions and write to you directly, asking you to remove them from your mailing list. It’s just plain good sense to do it for them, rather than going back and forth with instructions on how and why they should do it themselves.

NPP7 – Identifiers

You are required to use your own means, rather than government identifiers such as Medicare numbers, for identifying people. This ensures that government identifiers don't become a *de facto* system of identification in the private sector.

NPP8 – Anonymity

Give people the option of remaining anonymous when dealing with you, particularly on your Web site.

Look at each of the places where you collect personal information on your Web site, and consider whether you are asking for too much information. Start by considering the *minimum* amount of information required, and then find a reason for each additional piece of information.

For example, suppose you offer free registration for site visitors to get to a certain part of your Web site. The minimum information required is probably a user name and/or a password, and this allows the person to remain anonymous. You can then ask for other optional information – for example:

- You could reasonably ask for an e-mail address to keep them informed of updates.
- Perhaps you could reasonably ask for their name, if you intend to personalise the site for them.
- You could ask for other information to assist you in personalising the site.
- Finally, you could ask for other demographic information for marketing purposes.

NPP9 – Transborder data flows

This principle is intended to give personal information a similar level of protection outside Australia.

The Internet is a global medium, and you might have personal information stored outside Australia. In particular, consider these services, which are commonly supplied by non-Australian organisations:

- Web site hosting
- Mailing list servers (sometimes – incorrectly – called “listservs”)
- Credit card payment gateways

NPP10 – Sensitive information

The Privacy Act defines some information as “sensitive information”. It includes information or opinion about an individual’s racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual preferences or practices, criminal record or health information about an individual.

Sensitive information is given greater protection by the law. In general, you cannot collect this information without consent, although there are some exceptions.

If you deal with sensitive information, consult other sources for more information.

How can I find out more?

The best source for finding out more about the legislation is the Federal Privacy Commissioner's Web site at www.privacy.gov.au. You can download and read the NPPs themselves as they appear in the legislation, Information Sheets explaining them in more detail, and the latest news and updates.

In particular, you can read Information Sheets on these topics:

- Overview of the Private Sector Provisions
- Openness
- Access
- Access and the Use of Intermediaries
- Security and Personal Information
- Unlawful Activity and Law Enforcement
- Contractors
- Handling Health Information for Research and Management
- Application of the NPPs to Information Already Held
- Privacy Codes
- Coverage of and Exemptions from the Private Sector Provisions

Appendix: Sample Privacy Policy

This is the First Step Communications privacy policy, which is accessible from every page of our Web site www.firststep.com.au.

Feel free to copy this for your own use. However, we don't claim that it will suit your requirements, so we strongly recommend that you seek independent legal advice.

Privacy Policy

We know that your privacy is important to you, so it's important to us as well.

You can read the full details of our privacy policy below. As a quick summary:

- We only ask for personal information that we require.
- We'll tell you what information we have recorded about you.
- If you would like any personal information changed or deleted, just ask.

Who we are

This Web site is operated by First Step Communications. Our postal address is 8 Windich Place, Leederville WA 6007, Australia. You can reach us via e-mail at info@firststep.com.au or by telephone at +61 8 9444 1225.

What we know about you

When you visit our Web site, our Web server automatically records some *general* information about your visit, but does **not** recognise or record any *individual* information about you. The information we record and use for statistical purposes is:

- Your server address
- The date and time
- The pages accessed and documents downloaded
- The previous site visited
- The type of browser used

We can only identify you personally if you give us this information voluntarily.

We use a cookie to control pop-up windows, so that we don't annoy you with lots of pop-up windows every time you visit the site.

If you visit the site using one of our affiliate's links, we use a cookie to keep track of your visit, so that we can correctly pay the affiliate a commission if you make a purchase.

Your e-mail address

We do **not** know your e-mail address unless you give it to us. We only record your e-mail address if you send us a message, either directly or by signing up to our newsletters or on-line courses. We will use it only internally within the organisation, and will not disclose it to other organisations without your permission.

If you have given us your e-mail address, but do not want to receive e-mail from us in the future, please let us know by sending us e-mail at the above address.

How we use this information

We use this information to improve the content of our Web site and analyse what pages people visit, and to keep in touch with you. If you join [G'day Australia](#), we also use your information to customise the content of our Web site for you.

Who has access to your information?

We use this information internally and share it with other people or organisations who need to know it as part of working with us in our normal business activities (e.g. sub-contractors). When we share this information with others, we require them to sign an agreement to keep this information private.

We do **not** share your personal information with others except under these conditions, and we do **not** disclose or sell your personal information to others for use in mailing lists or databases.

Future Variations

If our information practices change at some time in the future we will post the policy changes to our Web site to notify you of these changes and provide you with the ability to opt out of these new uses. If you are concerned about how your information is used, you should check back at our Web site periodically.

Corrections

Upon request, we'll tell you what information we have recorded about you. For your own protection, we generally ask you to make this request in writing, so that we can verify your identity (E-mail is too easy to forge!)

If any of the information is incorrect, or you want us to remove all information about you, please contact us and we'll amend it promptly.

If you feel that this site is not following its stated information policy, please contact us at the above addresses or phone number.

In general, we value your privacy, and will only continue to correspond with you if either:

- you give us your e-mail address or postal address for this express purpose (for example, if you sign up to our newsletters or on-line courses, or request information about our products and services); or
- we have an existing business relationship (for example, you have bought our products or services).

In any case, if you do not wish to receive such mailings in the future, please let us know by sending us e-mail at the above address or writing to us at the above postal address.

More Information

If you would like to know more about on-line privacy, visit [The Australian Privacy Commissioner's Web site](#)