



Government of South Australia

Privacy Committee
Of South Australia

Privacy Guidelines for South Australian Government World Wide Websites

Guideline

January 2001

Version 1.0

Table of Contents

Introduction	3
Contact.....	3
Guideline 1	4
Privacy Statement.....	4
Guideline 2	4
Clickstream Data and Cookies.....	4
Collection of Personal Information via Websites	5
Guideline 3	6
Security	6
Guideline 4	7
Access and Correction of Personal Information	7
Guideline 5	7
Publication of Personal Information on a Website	7

© 2007 Government of South Australia

This Guideline may be copied for use by South Australian Government Agencies and Local Government Authorities and for reasonable study or research purposes. No part of this Guideline may be reproduced or distributed for profit or gain or for any other purpose without the written permission of the Manager [Director] of State Records of South Australia.

Introduction

These guidelines have been developed to assist South Australian Government agencies to develop a Privacy Statement for inclusion on their websites. The guidelines were issued by the Privacy Committee of South Australia. The guidelines are based on the Federal Privacy Commissioner's *Guidelines for Federal and ACT Government World Wide Websites*, and have been re-modelled to conform to the South Australian Government's Information Privacy Principles (IPPs).

When developing web and electronic service delivery strategies, agencies must consider the relevant privacy implications involved in transmitting, soliciting and collecting personal information. It is the responsibility of each agency to ensure that they comply with the IPPs. A copy of the IPPs can be found in *Premier and Cabinet Circular No. 12* (available at <http://www.premcab.sa.gov.au/pdf/circulars/Privacy.pdf>) and should be referred to when reading these guidelines.

Applications for exemption from compliance of one or more of the IPPs must be made in writing to the Privacy Committee of South Australia.

Contact

Contact in relation to these Guidelines can be made with the following State Records' staff:

- Manager, Freedom of Information and Privacy
- Executive Officer, Privacy Committee of South Australia

The above staff can be contacted at:

State Records of South Australia

GPO Box 1072

ADELAIDE SA 5001

Phone: (08) 8204 8786

Fax: (08) 8204 8777

Email: privacy@saugov.sa.gov.au

Guideline 1

Agency websites must incorporate a prominently displayed Privacy Statement that states:

- what information is collected;
- for what purpose;
- how this information is used; and
- if it is disclosed and to whom,
- and addresses any other relevant privacy issues.

Privacy Statement

State Government agencies must include a Privacy Statement which states the information collected from individuals, how the information it is used and if it is disclosed. Statements of this nature are now considered to be best practice.

Guideline 2

Agencies that solicit or collect personal information via their websites must comply with IPPs 1-3.

Agency website privacy statements should include a statement regarding this collection which complies with IPP 2. Where an online form is used to collect personal information the statement should be on the same page as the form or prominently linked to it.

Collection of information for the purpose of mailing lists etc, should be on an “opt-in” basis only.

Clickstream Data and Cookies

The IPPs define personal information as "...information about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion." Some information collected by website hosts about individuals visiting the site will not in itself identify the individual. This is sometimes called "clickstream data" and consists of information automatically collected and logged due to the nature of the communications protocols. The following text is an example of the Federal Privacy Commissioner's

website Privacy Policy (available at <http://www.privacy.gov.au/policy/index.html>) and sets out the clickstream data collected:

“Our service provider makes a record of your visit and logs the following information for statistical purposes – the user's server address, the user's top level domain name (eg. .com, .gov, .au, .uk etc.), the date and time of the visit to the site, the pages accessed and documents downloaded, the previous site visited and the type of browser used. No attempt will be made to identify users or their browsing activities except, in the unlikely event of an investigation, where a law enforcement agency may exercise a warrant to inspect the service provider's logs.”

Even though clickstream data may not in itself identify individuals, and so may not be personal information as defined in IPPs, it is recommended, in the interests of transparency, that website Privacy Statements state what clickstream data is collected.

Cookies can also be used to track individuals' activities on websites. Like clickstream data, cookies may not conform to the definition of personal information within IPPs, however many net users consider cookies to be intrusive. If a website uses cookies it is recommended that the Privacy Statement indicates that they are used and for what purpose.

Collection of Personal Information via Websites

Some agencies may collect e-mail addresses when individuals e-mail the agency via the website. Agencies may also use electronic forms to solicit personal information related to the agencies' functions. This will become more widespread as agencies employ the Internet for Electronic Service Delivery. Where agencies solicit and collect personal information via their websites, they must comply with the collection principles - IPPs 1-3.

IPP 1 requires that personal information not be collected by unlawful or unfair means and that the information should not be collected unnecessarily. IPP 2 makes similar requirements for when personal information is solicited by the collector. To comply with the collection principles, agencies should not collect or solicit personal information via their websites that would be unlawful, unnecessary or unrelated to their functions. Collection should not be unfair or unreasonably intrusive.

IPP 2 also requires agencies to provide notice to individuals where any personal information is solicited from the individual concerned. The notice should cover all those matters addressed by IPP 2, namely the purpose for which the information is being collected (including if the information is to be published), the legal authority for the collection if it is authorised or required by or under law and any usual disclosures made by the agency. If an agency is collecting personal information, for example for a mailing list, it should be collecting information on an “opt-in” basis, with the onus of gaining the individual’s permission lying with the agency.

IPP 3 requires that agencies do not to collect personal information that is inaccurate, irrelevant, out of date, incomplete or excessively personal.

An example of part of a Privacy Statement for a site that collects e-mail addresses follows:

We will only record your e-mail address if you send us a message. It will only be used for the purpose for which you have provided it and will not be added to a mailing list. We will not use your e-mail address for any other purpose, and will not disclose it, without your consent.

Guideline 3

When personal information is collected via an agency website it should be done by sufficiently secure means. Individuals should be provided with alternative means of providing personal information to the agency, other than via the website. The Privacy Statement should address security issues where appropriate.

Security

IPP 3 requires agencies to ensure that records containing personal information are protected by such security safeguards as are reasonable in the circumstances to take care against loss, unauthorised access, use, modification, disclosure and other misuse.

Agencies must ensure that their internal networks and databases which contain personal information are sufficiently protected from unauthorised access via their website and any Internet connection. Firewall technology is often used to protect internal networks from the web.

When agencies solicit or collect information from individuals using electronic forms or e-mail, they should make it clear to the individual the risks associated with using the Internet as the transmission medium and notify the individual of any other options there are for providing the information. For example, the individual may prefer to use the telephone or provide a response on paper.

If any security measures such as encryption are used, information regarding these should be provided to the individual. For example, the agency may include a hyperlink to a brief statement about Internet security and, if they use encryption, to a statement about the product used and the level of protection it provides.

Guideline 4

The Privacy Statement should give details on how members of the public can apply for access to their own personal information in accordance with the *Freedom of Information Act 1991*, including their rights to apply to correct personal information that is out of date, incorrect or misleading.

Access and Correction of Personal Information

IPP 5 states that individuals are entitled to access to personal information held by the State Government in accordance with the *Freedom of Information Act 1991*. IPP 6 refers to individuals' right to apply to correct personal information that is out of date, incorrect or misleading in accordance with the *Freedom of Information Act 1991*.

Guideline 5

Where agencies are considering the publication of personal information regarding individuals on the web they should be sure that this complies with IPPs 8 & 10.

Publication of Personal Information on a Website

Agencies may publish personal information if it is collected for the purpose of publication and the collection complies with the IPPs. If the personal information was not collected for inclusion in a publication, it may only be published if allowed by one of the exceptions to IPPs 8 and 10 (which respectively limit the use and disclosure of personal information). IPP 8 (a) allows the use of personal information for another purpose if the individual

concerned has consented to the new use. IPP 10 (a) allows disclosure of personal information where the individual concerned has consented to the disclosure. It is important, where consent for publication is sought, that it is informed consent.

The individual should be given to understand that if their personal information is published on the web it will be accessible to millions of users from all over the world, and that their information can be searched for, using an identifier such as the individual's name, and that their information can be copied and used by any web user. Most importantly, the individual should be made aware that once their personal information has been published on the web, the agency has no control over its subsequent use and disclosure.

There may also be instances where personal information is incidentally or accidentally published on the web. Personal information may be included in documents that are published on the web. It is recommended that documents be carefully checked before being published on the web and any unnecessary personal information removed.

Staff information

The staff of State Government agencies are entitled to the same protection, afforded by the IPPs, as agency clients. However staff in senior positions, or positions of public contact, would normally expect their contact details to be publicly available in some form. These staff members should be advised if their personal information is published on the web.

Other staff, however, may not expect their personal information to be published on the web or in another form. There have been instances where agencies have published entire staff telephone lists on their websites.

It is easy to download or print a staff list that is made available on the web. The publication and easy accessibility of this information may place staff at risk of receiving unsolicited e-mail (spam) and unwelcome attention from a range of people and organisations.

Publishing a staff list on the web may place staff in a position where they are subject to scrutiny by people with whom they would not normally choose to share their personal information. The publication of information such as staff classifications may make the

information even more interesting to third parties as the salary range associated with these classifications is publicly available information.

There may also be dangers to particular staff in publishing their personal information on the web. Individuals may be placed at risk of harassment, particularly if their work involves contact with members of the public. For personal safety reasons individuals may not wish to have their work contact details published.