Government of South Australia

Privacy Committee
Of South Australia

Privacy Guidelines for South Australian Government Websites and Online Applications

Publication

April 2014

Version **1.2**

Executive Officer
Privacy Committee of South Australia
c/o State Records of South Australia
GPO Box 464
ADELAIDE SA 5001
Phone (08) 8204 8786
privacy@sa.gov.au

Table of Contents

Introduction

These guidelines have been developed to assist South Australian public sector agencies to understand how the Government's Information Privacy Principles Instruction (IPPI) applies to agency websites. It also aims to assist agencies to develop privacy statements that explain how the agency handles any personal information collected via its websites, mobile applications and social media services.

Why is a privacy statement important? The collection of personal information by a website, a mobile application or a social media site is not always obvious. Some information may be collected overtly, such as when an individual is asked to provide information directly, other information may be collected covertly through the agency's web server or through the use of cookies. It is also not always clear what will happen to the information once it is collected. It is important that users understand what information an agency is collecting about them and what the agency will do with it. This allows the user to make an informed decision about the extent to which they transact with the agency. Ultimately, being open and transparent about the way the agency handles personal information will promote trust in the agency's practices and provide users of the agency's website a greater level of control over how their personal information is used.

These guidelines are issued by the Privacy Committee of South Australia. They replace the *Privacy Guidelines for South Australian Government World Wide Websites* version 1.1, issued by the Privacy Committee of South Australia in January 2001.

The Information Privacy Principles Instruction

The IPPI is an instruction of Cabinet, issued as *Premier and Cabinet Circular No 12.* It is the responsibility of the Principal Officer of a public sector agency to ensure that their agency complies with the IPPI. The IPPI sets out ten information privacy principles (IPPs) that guide the way South Australian government agencies collect, store, use and disclose personal information[1]. These Guidelines should be read in conjunction with the IPPI.

Under the IPPI, the term 'personal information' means:

> *Information or an opinion, whether true or not, relating to a natural person or the affairs of a natural person whose identity is apparent, or can reasonably be ascertained, from the information or opinion.*

Personal information is, therefore, any information that can be linked to an identifiable living person. This could include a document, an identifying number, a photograph or video. It could include information detailing the person's name, address, date of birth, financial or health status, ethnicity, gender, religion, alleged behaviour, licensing details, or a combination of such details. The important question to ask in determining whether information is personal information is whether it can identify a particular individual.

[1] A reference to a particular IPP in this guideline is a reference to the relevant subclause of the IPPI. For example, IPP 2 is a reference to Clause 4 (2) of the IPPI.

Privacy Statement or Privacy Policy?

Under IPP 2 there are a number of basic things that an agency must tell an individual before collecting that individual's personal information. They include the purpose for collecting the information, whether the collection is authorised or required by law and the agency's usual practices in terms of disclosure. This information is only the minimum that an agency must tell an individual when collecting their personal information. However, it is good privacy practice for an agency to be as open and transparent as possible about the way in which it will handle personal information and comply with the IPPI.

The agency may fulfil these obligations by publishing a privacy policy outlining how it will handle personal information. The challenge for the agency is to provide simple, clear and understandable information that is practicable in the circumstances. What might be practicable in collecting information via an online form may not be practicable for a transaction over the phone or online application. One way of approaching this challenge is to adopt a Layered Privacy Policy[2] approach. A layered approach involves the use of a condensed privacy statement or notice at the point of each transaction with an individual and then having a separate comprehensive privacy policy that the individual can access if they require further more detailed information. A privacy statement can then be tailored to the specific transaction. For example, a privacy statement on an agency's website may describe the ways in which the agency will collect and handle information via the website but it could also provide a link to the agency's privacy policy which outlines all of the agency's practices in the handling of personal information.

Alternatively, an agency may decide to adopt a single policy to serve all purposes. Consideration should be given to how practical it is to provide a full privacy policy to support all transactions on the agency's website. Particular consideration should be given to the length and layout of the statement, the information presented and the space available.

Clarity and accessibility of Privacy Statements

The aim of an agency privacy statement is to help an individual to understand how the agency will handle their personal information. It, therefore, may be relied upon by an individual in determining whether or not they will transact with the agency. For this reason, it is important that the agency's privacy statement is both clear and accessible. The clarity of the statement can be measured in terms of its readability. If a privacy statement is too long or complex, or full of jargon or technical terms, there is a likelihood that the individual will either not read it or will have some difficulty in understanding what it means. A privacy statement should err on the side of stating the obvious.

Privacy statements should be accessible, that is, both easy to find on the website and accessible to all individuals. Consider the accessibility of the privacy statement in the

[2] The Layered Privacy Notices format was endorsed by Data Protection & Privacy Commissioners in 2003, further developed in the Berlin Memorandum and endorsed in Opinion WP 100 by the Article 29 Committee of European Data Protection Commissioners.

design of the website. Place a link to the statement on each page. Consider also whether the privacy statement is accessible to as broad an audience as possible. This includes people with disabilities who may use assistive technology to read or hear content. Web privacy statements should comply, at minimum, with Conformance Level A of accessibility in the Web Content Accessibility Guidelines Version 2.0.

The Content of the Privacy Statement

An agency's website should incorporate a privacy statement outlining its general practices in handling personal information and complying with the IPPI. If the website is to collect personal information at any stage, the privacy statement must include, at minimum, the information as described in IPP 2 that the agency is required to tell an individual before, or as soon as practicable after, collecting their personal information. The statement should also include information about any clickstream data collected or information collected via the websites' use of cookies. (See page 7)

In summary, the statement should include:

- What information is collected
- For what purpose
- If it is authorised or required by or under law, that it is so authorised or required
- How this information is to be used
- If it is to be disclosed, to whom it is to be disclosed,
- How a person can access or correct any information the agency collects about them
- Any automatic or covert collection of information through cookies or clickstream data
- Any other relevant privacy issues.

Collection of personal information (IPPs 1-3)

Agencies may collect personal information in a variety of ways, such as when a person contacts the agency by telephone, email or letter, or via its website. The collection of information via agency websites can also vary from no collection to the collection of sensitive personal information depending on the types of transactions the agency conducts online. Collection can occur through various means including a web form, an online payment gateway or an online survey.

IPP 1 requires that personal information not be collected by unlawful or unfair means and that the information should not be collected unnecessarily. To comply with the collection principles, agencies should not collect or solicit personal information via their websites in a way that would be unfair, unlawful, unnecessary or unrelated to their functions or activities. In preparing a privacy statement, an agency should consider carefully the information it collects via its website and the purposes for which it is collected. It must consider whether it is necessary for one or more of the agency functions or activities.

IPP 2 requires that before an agency collects personal information from an individual or, if that is not practicable, as soon as practicable after it has collected the information, the agency must tell the individual:

- the purpose for which the information is being collected, unless that purpose is obvious;
- if the collection of the information is authorised or required by law – that the collection of the information is so authorised or required; and
- in general terms, of its usual practices with respect to disclosure of personal information of the kind collected.

Purpose for collection

The agency privacy statement should include enough information about how the personal information to be collected will be used, and what it will be used for, to enable an individual to make an informed decision about whether he or she will proceed with the transaction with the agency. The relevant functions of the agency and the purposes for collecting personal information online should be outlined in simple terms. An agency should consider carefully the information it collects and why that information is required for its functions or activities.

Authorised or required by law

The agency should outline any personal information that it is required or authorised by law to collect. If an individual is compelled by law to provide their information this should be made clear in the privacy statement. The agency should avoid general statements about its lawful obligations and instead state the specific legislation or legal basis for the collection.

Usual practices for disclosure

The agency should be as clear and as specific as possible about any third parties to whom it discloses personal information and for what purpose. For example, if an agency is collecting personal information to facilitate an online payment for an agency service it should be made clear that it will be disclosing this information to its payment service providers. If the agency has a need to disclose personal information in response to requests from law enforcement bodies, it should make this clear in its statement. If the agency is authorised or required to disclose personal information collected on its website to other government agencies, the names of those agencies and the reasons for disclosing information to them should be provided. The agency should provide details of the limits of any such disclosures and how they comply with the provisions of IPP 10.

If an agency is collecting personal information that it plans to disclose to a private sector organisation for advertising or marketing purposes, it should be collecting information on an "opt-in" basis with the individual's informed consent[3].

IPP 3 requires that agencies do not collect personal information that is inaccurate or, having regard for the purposes of collection, is irrelevant, out of date, incomplete or excessively personal.

[3] Informed consent means that the individual is told and, could reasonably be expected to understand, that the personal information will be published online.

Cookies and clickstream data

The IPPI defines 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 by the web server which provides useful information about a user's online experience without identifying them.

Types of clickstream data can include:

- server address
- top level domain name (for example .com, .gov, .au, .uk etc.)
- the date and time of your visit to the site
- the pages you accessed and documents downloaded during your visit
- the previous site you visited
- if you've visited our site before
- the type of browser used.

Even though clickstream data may not in itself identify individuals, and so may not be personal information as defined in the IPPI, it could be linked to a person at a later date, for example in a subsequent law enforcement investigation. It is therefore recommended, in the interests of transparency and good privacy practice, that privacy statements include what clickstream data is collected.

Cookies can also be used to track individuals' preferences and visiting patterns on websites. Like clickstream data, information collected via cookies may not conform to the definition of personal information within the IPPI, however many net users consider cookies to be intrusive. They may collect information that could be linked to an individual's identity, such as their computer ID. If an agency website uses cookies it is recommended that the privacy statement indicates the purposes for the agency using cookies.

Anonymity and pseudonymity

It is good privacy practice for an agency to provide members of the public with the option of dealing with it anonymously or through the use of a pseudonym, where it is reasonable and practicable to do so. For example, agencies should consider whether it needs members of the public to identify themselves if they are merely seeking general information, making a general enquiry or completing an online survey through the website.

In some cases it is not practicable or reasonable for an agency to deal with a member of the public anonymously, for example if a member of the public is seeking a formal response to a complaint they have made about the agency.

Agencies should also be aware of the requirements of third party websites, including social media websites, which may not allow anonymous use of the website or use of the website using a pseudonym.

Storage of Personal Information (IPP 4)

IPP 4 requires that agencies take such steps as are, in the circumstances, reasonable to ensure that personal information in its possession or under its control is securely stored and is not misused.

At minimum, reasonable steps would include meeting the existing standards for information security management in the South Australian Government. These standards are outlined in the Information Security Management Framework. Security of information on an agency's website is one part of the wider obligation of an agency to secure its data. Websites provide a direct link between an agency and the outside world. Agencies should pay particular attention to the security associated with their website to ensure that any internal networks and databases which contain personal information are sufficiently protected from unauthorised access via their website.

When agencies solicit or collect information from individuals using electronic forms or email, it should be made clear to the individual the risks associated with using the Internet and the individual should be notified of any other available options for providing the information.

Access and Correction (IPP 5 and 6)

An agency's privacy statement should include advice about an individual's entitlement to access and correct his or her personal information. The agency may have an administrative process for accessing and correcting particular information, such as permitting an individual to update their contact details via a web form.

IPP 5 provides that where an agency has in its possession or under its control records of personal information, the record-subject should be entitled to have access to those records in accordance with the *Freedom of Information Act 1991*(FOI Act). The FOI Act gives an individual a legal right to apply for access to information concerning their personal affairs and in most cases access is provided under the Act.

IPP 6 provides that an agency that has in its possession or under its control records of personal information about another person it should correct it in accordance with the FOI Act so far as it is inaccurate or, having regard to the purpose of collection or to a purpose that is incidental to or connected with that purpose, incomplete, irrelevant, out of date, or where it would be misleading.

An agency's privacy statement should include details about any normal administrative process for providing access. It should also outline an individual's right to access or correct their personal information in accordance with the FOI Act. The statement should provide information, or a link to such information, on how the individual might exercise that right.

Publication of Personal Information on Agency Websites (IPPs 8-10)

Where an agency is considering the publication of individuals' personal information on its website it should be sure that the publication complies with IPPs 8 and 10.

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 publication, it may only be published if allowed by one of the exceptions to IPP 10. This includes where the individual would reasonably expect the agency to disclose the information for a secondary purpose related to the primary purpose of collection (IPP 10(a), or where the individual has expressly or impliedly consented to the disclosure (IPP 10(b).

Where consent for publication is sought, it is important that the individual's consent is informed. Informed consent would generally mean that the individual is told, and could reasonably be expected to understand, that the personal information will be published on the web. The individual should be told that it will be accessible to users from all over the world, and that their information could be searched, 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 a risk that personal information is incidentally or accidentally published on an agency's website. Personal information may be included in documents that are published on an agency's website. It is recommended that documents be carefully checked before being published on an agency web site and any unnecessary personal information be removed or redacted.

Public Registers

In some cases an agency is lawfully obliged to publish certain information, for example information held in a public register. An agency may choose to publish this information on its website. There are many examples of online public registers including searchable registers of licensed tradespersons or lands titles records. Agencies should consider the possible impacts of publishing a public register online, including the potential for the information on the register to be aggregated or cross-matched with other publicly available information. It is recommended that an agency undertake a Privacy Impact Assessment[4] prior to publishing a public register online.

The agency could consider:

[4] The Privacy Committee recommends that agencies follow the Office of the Australian Information Commissioner's Privacy Impact Assessment Guideline, which can be accessed at http://www.oaic.gov.au/publications/guidelines/Privacy_Impact_Assessment_Guide.html.

- What discretion it has on the extent of information published on the register. Is the information published from the register limited to what is required by law? Is other information included that the agency is not required to publish.
- The limits it can put on access to the register by external search engines.
- Whether there is a need to restrict bulk access to the register and limit access to single unit searches.
- Whether registration is required to access the register and records kept this access.
- What secondary uses the register may be used for, such as direct marketing or use by disreputable persons to locate victims of, or witness to, criminal actions
- Whether there is any scope or discretion to suppress the records of individuals with a genuine reason for fearing for their life or safety (such as victims of domestic violence).

An agency should consider seeking legal advice prior to publishing a public register online. Further general advice can also be sought from the Privacy Committee.

Staff Information

Employees of the Government of South Australia are entitled to the same protection afforded by the IPPI, as agency clients. However, staff in executive positions, or positions of public contact, would reasonably expect their contact details to be publicly available in some form. These staff members should be advised if their personal information is to be published on an agency website.

Other staff, however, may not expect their personal information to be published on an agency website or in another form. For example, there have been instances where agencies have published entire staff telephone lists on their websites. The publication and accessibility of this information may place staff at risk of:

- receiving unsolicited e-mail (spam)
- being harassed
- physical danger

An agency should carefully consider any publication of staff information on its website. It should consult staff about the potential impact of such publication prior to determining whether it is reasonable to publish the information.

Online Applications (Apps)

Online applications or apps, as they are more commonly known, are applications that have been developed specifically for use on smartphones, tablets, computers and other mobile computing devices[5]. The term 'app' has been in use for many years but more recently has become the popular short form for applications developed for smartphones and other mobile computing devices.

Apps and the IPPI

If an agency is collecting personal information via an online app, that collection must comply with the IPPI. As previously outlined, IPP 2 requires an agency to tell the individual *before* it collects their personal information the purposes for the collection, whether it is authorised or required by law and its usual practices for disclosure of personal information.

Apps are often designed for small screens and by design are limited in the amount of information that can be displayed on any one particular page. However, that should not be a barrier to agencies meeting the requirement of IPP 2. Short privacy statements can usually be accommodated if considered early in the design of the agency app.

An agency should develop a prominent privacy statement for each app it develops that includes details about the information specifically collected by the app and the information required under IPP 2. Alternatively, an agency could include information about collection via its apps in a website privacy statement or in its privacy policy and provide a prominent link to that information in its app. Whichever approach the agency decides to take it should make sure that every possible step is taken to inform app users of the minimum information it is required to provide under IPP 2.

The range of information collected by mobile apps varies considerably depending on the functions of the app. While not all information collected by a mobile app will fall within the definition of personal information under the IPPI, it may still include information that can be linked back to the user in combination with information available from other sources or through other web applications. Agencies should take a cautious approach in determining whether any information collected via an app is personal information, with a full understanding of the risks to the user, particularly if it is intended that information will be disclosed to a third party.

[5] Wikipedia, see http://en.wikipedia.org/wiki/Mobile_app.

Things to consider when developing Apps[6]

An agency should consider the privacy impacts of the collection of user information in the development of apps. The following actions will help agencies ensure that they both comply with the IPPI and follow good privacy practice.

Action	IPP
Undertake a Privacy Impact Assessment as part of app planning and development. Consider and map the flow of personal information. This will help to identify privacy vulnerabilities in a systematic way.	
Consider what personal information is essential for the app's function. Consider whether the app needs to collect and use personal information at all to function. If it does, collect only as much personal information as you need to enable the app's function. Do not collect personal information just because it may be useful or valuable in the future.	IPPs 1-3
Tell people how the app will use personal information and who it will be disclosed to. During the installation, tell users what personal information the app is collecting, what it will be used for, and who it will be shared with. It can be difficult to communicate this information effectively in the small screen environment. Consider strategies for giving an effective notice, such as layering information, putting important information up front and more detailed information available via a link to the agency's privacy statement or policy. Consider using graphics, colour or sound to draw attention to notices.	IPP 2
Have a clear and accessible privacy policy. Ensure you have a clear and accessible policy which enables users to evaluate what you propose to do with their personal information. Users should be able to access this information before deciding whether to download the app. Make sure your policy lets users know how they can access or amend their personal information, how they can delete the app or their subscription to the app, and what will happen to personal information already collected and stored.	IPP 2

[6] In developing this guidance the Privacy Committee acknowledges the Canadian resource - 'Seizing Opportunity: Good Privacy Practices for Developing Mobile Apps' and the Queensland Information Commissioner's Guidance: 'Privacy and Mobile apps'. Further acknowledgement of sources is listed at the end of this guideline.

Consider how personal information will be stored and secured. Agencies must take steps to secure personal information from misuse. Ensure that the storage and security of any personal information collected through the mobile app is well planned, and that appropriate controls are in place on both the mobile device and backend systems that will store personal information. Security safeguards should be appropriate to the sensitivity of the information. Agencies should consider the South Australian Government Web Application Security Standards and the Information Security Management Framework.	IPP 4
Only use and disclose personal information in permitted circumstances. Agencies may need to use and disclose personal information for an app to function. For example, location data may be required to deliver certain functions in a navigation app (such as public transport apps). Agencies may need to share personal information with another entity to provide the services offered by the app. Apps should generally only use personal information for the purpose it was collected, and only disclose it to the individual it is about, except in limited circumstances. Agencies should monitor apps to ensure personal information is only used and disclosed in ways that are permitted by the IPPI and in accordance with their privacy statement or policy.	IPPs 8-10
Consider whether contractors will be engaged to perform any services which involve personal information. If an agency plans to engage a contracted service provider to perform services connected with the development or delivery of an app, these providers will need to comply with the IPPI as required by their contractual obligations[7].	Clause 5
Consider the end of life of personal information. Ensure that a plan exists for when the app is deleted, or subscription ends, taking into account public records and other legal obligations including those under the *State Records Act 1997*.	IPP 4
Plan for breaches and complaints. Agencies should develop specific procedures for dealing with privacy breaches and complaints associated with their mobile apps. [8]	

[7] Further information about contracting and the IPPs can be found in the Contracting and the Information Privacy Principles information sheet.

[8] The Office of the Chief Information Officer must be contacted in the case of a privacy breach that involves electronic information.

Social Media

In addition to a standard agency website, many agencies utilise social media services such as Facebook, Twitter, YouTube, Instagram, LinkedIn, Google+ and Flickr to connect and interact with the public and other stakeholders. Social media services can be a cost effective way for an agency to communicate and interact with the community. They can be used to promote greater transparency of government services and encourage community engagement.

However, agencies should be mindful that there are privacy concerns that need to be addressed when using a social media service, particularly if the agency is collecting personal information as a result of using a particular service. An agency's obligations under the IPPI may extend to its collection of personal information via a social media service. It is, therefore, important that an agency understands and addresses its obligations under the IPPI and any other privacy impacts when establishing a presence on a social media service. Agencies should specifically consider IPP 2 and the information they are required to provide individuals before they collect their personal information.

Agencies should consider developing a privacy statement that can be used on social media sites. In some cases, due to the design of the social media site, it may not be possible to include a privacy statement directly on the social media service. In these instances, consideration should be given to providing a link back to the agency's privacy statement or policy hosted on the agency's website.

Particular considerations for Social Media sites

Action	IPP
Privacy risks should be assessed for each social media service before deciding to use it. This could be in the form of a Privacy Impact Assessment (PIA). Social media services are often public forums and as such an agency should take great care about the information they post on a social media site.	
The PIA should determine whether the agency is likely to collect personal information in the use of the social media service (e.g. will it seek public feedback, accept enquiries or use a user's profile information). The assessment should also consider the risk of inadvertent disclosure of personal information and how this might be mitigated.	
Do not collect more information than is necessary for the agency's functions or activities.	IPP 1
If collecting personal information ensure that users of the agency's social media site are provided access to a privacy statement or policy that, at minimum, complies with the requirements of IPP 2.	IPP 2
If collecting personal information from the social media site the agency should take reasonable steps to ensure the information is accurate, complete and up to date. An agency should not collect information that is excessively personal.	IPP 3

An agency's privacy statement should explain to individuals the limits of the agency's control over information on the social media service. As most social media services are run by private companies and foreign entities, agencies should address any information security risks before agreeing to use the service. If an agency collects information from the social media service and holds it in its own information systems and databases it must secure that information in line with IPP 4. Consider the agency's obligations under the Information Security Management Framework in utilising the social media service.	IPP 4
An agency should consider how it manages any official records created during the use of the social media service. This includes recording any decisions made or transactions undertaken with individuals via the social media service.	
Do not disclose personal information on a social media service unless the disclosure complies with IPP 10. In most cases, disclosure of personal information should only occur with the informed consent of the individual to whom the information relates.	IPP 10

Further Information & Contact Details

A copy of the IPPI is available from the Department of the Premier and Cabinet website at http://dpc.sa.gov.au/premier-and-cabinet-circulars and should be referred to when reading this guideline.

If you would like more information about this guideline, you can contact State Records' Freedom of Information and Privacy hotline on (08) 8204 8786 or via the contact details below:

Privacy Committee of South Australia
c/o State Records of South Australia
GPO Box 464
ADELAIDE SA 5001
Email: privacy@sa.gov.au

Acknowledgements

In developing this guidance the Privacy Committee has utilised the significant work of other Australian and international privacy authorities on the issue of online privacy. This includes the following publications:

Guidelines for Federal and ACT Government Websites, Office of the Australian Information Commissioner, 2003.

Information Sheet: Social Networking, Office of the Victorian Privacy Commissioner, 2011.

Privacy and Mobile Apps, Office of the Information Commissioner Queensland.

Seizing Opportunity: Good Privacy Practices for Developing Mobile Apps developed jointly by the Office of the Privacy Commissioner Canada, the Office of the Information and Privacy Commissioner of Alberta and the Office of the Information and Privacy Commissioner for British Columbia.

Website Privacy – Guidelines for the Victorian Public Sector, Office of the Victorian Privacy Commissioner Victoria, 2004.