Accompanying Guide

A guide to completing Parts 3 to 5 of your Privacy Impact Assessment Report

privacy victoria

Office of the
Victorian Privacy
Commissioner

This document provides assistance to any person conducting a Privacy Impact Assessment. However this document is particularly aimed at people completing Parts 3 to 5 of the Privacy Victoria Template PIA Report.

For each privacy principle in Part 3, privacy right in Part 4 and other privacy issue in Part 5 of the Template PIA Report, this document provides tips to help you identify the risks, and develop strategies to mitigate those risks.

Not every risk listed here will be relevant to your project. Nor will every risk associated with your project be included here – you may uncover many other privacy issues. Also bear in mind that some risks affect more than one privacy principle.

This guide is only intended to prompt your own analysis and assessment.

COVER PHOTO: www.istockphoto.com

Table of Contents

Anonymity (IPP 8) – Part 3 of the Template PIA report

COMMON RISKS TO CONSIDER	IDEAS FOR MITIGATION STRATEGIES
Collecting people's identity details where it is not required.	Carefully consider: can you use information that does not identify a person? If you need to be able to delineate one client from another but don't really need to know their complete identity, could you use pseudonyms instead? See also Privacy Victoria, *Confirming Identity and Privacy: A Guide for Organisations*, Info Sheet 07.08, December 2008.
Collecting people's names and addresses in order to send them material.	Have material published on your website for people to download anonymously.
Smartcards can present a risk of collecting identifiable information that is not necessary.	Not all smartcards have to be personalised. Anonymity can be built in to the design phase in some circumstances.
De-identification poses the risk of re-identification.	Carefully consider: where personal identifiers are not used or have been removed, how readily can a person be re-identified?
For more ideas on risks and mitigation strategies associated with this Principle, see Privacy Victoria, *Guidelines to the Information Privacy Principles*, September 2006.	

Collection necessity (IPP 1.1) – Part 3 of the Template PIA report

COMMON RISKS TO CONSIDER	IDEAS FOR MITIGATION STRATEGIES
The risk your collection of personal information is unlawful.	You cannot collect personal information just because the person consents to give it to you. Seek legal advice to check that you have the lawful authority to operate this project in the first place. Document your legal authority in your PIA Report.
Collecting personal information without a clear purpose increases the risk of unauthorised uses and disclosures.	Ensure the purpose/s for which you will be collecting and using personal information have been clearly specified, and that there is a shared understanding of those purpose/s throughout the organisation. Document the purpose/s in your PIA Report.
The risk of collecting personal information in breach of IPP 1. (However if you are collecting health information, the rules are more stringent; see HPP 1.)	Check every piece or field of data you seek to collect. Remove anything that is not absolutely necessary. Document in your PIA Report why the remainder is necessary.
The risk that IT system design dictates what personal information is collected.	Ensure your privacy and business requirements dictate your system requirements, not the other way around. Avoid ending up with an IT system with fields that require unnecessary data, just in order to register people or process transactions.

Collection necessity (IPP 1.1) – CONTINUED

COMMON RISKS TO CONSIDER	IDEAS FOR MITIGATION STRATEGIES
Collecting more detail than you can justify can increase the risk of poor data quality. The more a person perceives a request for information as intrusive or unnecessary, the more likely they are to give false answers to protect their privacy.	Check every piece or field of data–can it be justified as necessary, proportionate, appropriate and not intrusive? Remove anything that is unnecessary, disproportionate or intrusive.
Collecting more detail than you need can increase the risk of data security breaches. Protecting the security of personal information is more difficult when it is routinely collected without due consideration.	Check every piece or field of data–can it be justified as necessary, proportionate, appropriate and not intrusive? Remove anything that is unnecessary, disproportionate or intrusive.
Collecting more detail than you need can increase the risk of identity fraud or theft.	If you need to know 'age' in order to provide age-appropriate services, ask for the person's age-range or year of birth, not their exact date of birth.
The routine collection of a person's home address raises particular privacy and safety concerns for some people.	Ask for a person's postal address only, unless you absolutely need to know their street address. Have a mechanism by which people can provide their home address but have access to that data particularly restricted.
The routine collection of a person's home telephone number raises particular privacy and safety concerns for some people.	Give people the option of providing contact numbers other than their home number. Have a mechanism by which people can provide their home number but have access to that data particularly restricted.
The risk you will be collecting superfluous personal information. For example, surveillance may collect personal information about persons other than the target.	Restrict your collections to only what is absolutely necessary, and include these in your privacy notice. This may include transaction data collected automatically (e.g. for audit purposes).
Cookies pose a particular risk of unnecessary collection of personal information.	Check whether you will be using cookies to log the IP address used when a client provides you with information via an online form; is this really necessary? If cookies are essential in order that an online transaction can proceed, avoid using persistent cookies, and use only session-based cookies. Include these in your privacy notice.
The risk of unnecessary collection when new materials are added to your website from time to time.	Develop a checklist for your website content managers, to check before they upload any new forms, surveys or other methods of collecting personal information online. The checklist should cover all the Collection and Anonymity principles.
The risk of community backlash if special sensitivities are not considered.	Consider community expectations. One way to do this is to conduct meaningful community consultation, which may identify community concerns that would otherwise be overlooked.
For more ideas on risks and mitigation strategies associated with this Principle, see Privacy Victoria, *Guidelines to the Information Privacy Principles*, September 2006.	

Method of collection (IPP 1.2) – Part 3 of the Template PIA report

COMMON RISKS TO CONSIDER	IDEAS FOR MITIGATION STRATEGIES
The risk of breaching privacy by using unjustifiably intrusive methods to collect personal information.	Consider other options for collecting the required information in less intrusive ways. Document the costs and benefits of each option. If a less-invasive option has been rejected, explain why in your PIA Report.
The risk of community backlash if special sensitivities are not considered.	Consider community expectations if you plan to use fingerprinting or other biometrics, audio or video recording, or location-tracking technology as a method of collection.
The risk of non-compliance with other legislation.	Check that your project will comply with your own enabling legislation, and any other applicable legislation such as the *Surveillance Devices Act 1999 (Vic)* and the *Telecommunications (Interception) Act 1979 (Cth)*.
The risk you will be disclosing personal information not previously identified as such. 'Disclosure' can encompass publishing information on the internet or in a public register, allowing researchers to access the information, or verbal discussions.	Check with all likely users of the data as to how they plan to disclose the data.
A collection could be considered 'unfair' if the person was under the impression that their personal information was required by law.	If you are required by law to collect some personal information, ensure this is differentiated from other information you are collecting at the same time for your own purposes. See further below under 'Collection notice'. If you are collecting personal information involving criminal records, also see Privacy Victoria, *Handling Criminal Records In The Public Sector*, Info Sheet 03.09, April 2009
For more ideas on risks and mitigation strategies associated with this Principle, see Privacy Victoria, *Guidelines to the Information Privacy Principles*, September 2006.	

Collection notice (IPP 1.3) – Part 3 of the Template PIA report

COMMON RISKS TO CONSIDER	IDEAS FOR MITIGATION STRATEGIES
The risk of non-compliance with this principle if you don't differentiate between mandatory and voluntary collections.	If you are required by law to collect some personal information, ensure this is differentiated from other information you are collecting at the same time for your own purposes. For example, a form could use the following key for each field or piece of data requested: # = this data is required under the X Act, * = this data is necessary to perform our function of Y, blank = optional / voluntary. Ensure the privacy notice explains the repercussions for each type of data if it is not supplied.
Privacy notice is not accessible to clients using alternate communication channels.	Ensure the privacy notice is consistent and accessible across all methods of collection, e.g. printed forms, online, and telephone discussions.

Collection notice (IPP 1.3) – CONTINUED

COMMON RISKS TO CONSIDER	IDEAS FOR MITIGATION STRATEGIES
Privacy notice is at the end of a multi-page online application form or survey.	Where the collection of personal information is spread across more than one web-page, ensure the privacy notice for that collection is available on the first page, and ideally also available as a link from every page.
People of a NESB may not understand the privacy notice.	Have your privacy notice translated into the community languages most appropriate for your client base. A generic community language privacy notice can be downloaded from www.lawlink.nsw.gov.au/privacynsw under 'Publications–Privacy Essentials'.
People with visual impairments may not be able to access the privacy notice.	Make your privacy notice available in Braille and/or suitable for use with adaptive technology such as screen readers.
People with limited capacity (e.g. people with an acquired brain injury or intellectual disability) may not understand the privacy notice.	Consult with disability experts to have your privacy notice communicated in other ways.
For more ideas on risks and mitigation strategies associated with this Principle, see Privacy Victoria, *Guidelines to the Information Privacy Principles*, September 2006.	

Direct collection (IPP 1.4) – Part 3 of the Template PIA report

COMMON RISKS TO CONSIDER	IDEAS FOR MITIGATION STRATEGIES
The risk your collection of personal information from another organisation is unlawful.	Consider the original purpose for which the other organisation collected the information, and whether the individuals affected would reasonably expect their information to be disclosed to you. You may need to ask the other organisation to amend its privacy notice, seek people's consent, or obtain specific legal authority for your project to proceed.
The risk your collection of personal information on behalf of another organisation is unlawful.	Seek legal advice to check that you have the lawful authority to collect personal information on behalf of another organisation.
Collecting personal information via a third party can increase the risk of poor quality data, because the affected person did not have the opportunity to check the data for accuracy.	Where direct collection is not possible, best practice is to ensure that the individual has provided authorisation for their personal information to be collected via another party.
Collecting personal information via a third party can increase the risk of complaints about secondary use or disclosure, because the affected person did not have the opportunity to challenge requested information, or your purposes for the information, as irrelevant.	Where direct collection is not possible, best practice is to ensure that the individual has been provided with a privacy notice.

Direct collection (IPP 1.4) – CONTINUED

COMMON RISKS TO CONSIDER	IDEAS FOR MITIGATION STRATEGIES
Although in some circumstances it would defeat the purpose of the collection if it was directly from the person (e.g. in the case of an investigation of the person), the practice of indirect collection could be seen as arbitrary if it is not standard procedure.	Be open about your practices; outline in your PIA Report and in a policy document the circumstances in which you will have to collect personal information about a person via other parties.
The risk that a 'consent' to indirect collection will not be valid.	Check the process by which you plan to seek consent. Ensure the consent will be truly voluntary (i.e. there will be no repercussions for individuals who refuse their consent), informed, specific, current and given by a person with the capacity to give or refuse their consent. If written consent cannot practicably be obtained, verbal consent should be recorded contemporaneously. For more advice about consent and capacity, see Privacy Victoria, *Guidelines to the Information Privacy Principles*, September 2006, under 'Key Concepts'.
For more ideas on risks and mitigation strategies associated with this Principle, see Privacy Victoria, *Guidelines to the Information Privacy Principles*, September 2006.	

Collection of sensitive information (IPP 10.1) – Part 3 of the Template PIA report

COMMON RISKS TO CONSIDER	IDEAS FOR MITIGATION STRATEGIES
The risk of non-compliance with this principle if you collect sensitive information without authority.	Sensitive information can only be collected if one of the conditions in IPP 10 is satisfied. Check carefully that you can meet one or more of those conditions–e.g. you have the person's consent, the collection is required under law, or another exemption applies.
The risk that a 'consent' to collect sensitive information will not be valid.	Check the process by which you plan to seek consent. Ensure the consent will be truly voluntary (i.e. there will be no repercussions for individuals who refuse their consent), informed, specific, current and given by a person with the capacity to give or refuse their consent. If written consent cannot practicably be obtained, verbal consent should be recorded contemporaneously. For more advice about consent and capacity, see Privacy Victoria, *Guidelines to the Information Privacy Principles*, September 2006, under 'Key Concepts'.
The unauthorised use or disclosure of sensitive information can result in discrimination against the person.	The best way to guard against unauthorised use or disclosure is to not collect the data in the first place. Check every piece or field of sensitive information to be collected–can it be justified as necessary, proportionate, appropriate and not intrusive? Remove anything that is not absolutely necessary.

Collection of sensitive information (IPP 10.1) – CONTINUED

COMMON RISKS TO CONSIDER	IDEAS FOR MITIGATION STRATEGIES
Questions about a person's "country of birth", "citizenship" or "language spoken at home" can be seen by respondents as a shorthand way of defining ethnicity, and are resented or seen as evidence of racial profiling.	Avoid asking these types of questions where possible. If you do need to ask them, explain why it is necessary, or clearly mark the questions as optional. If you want to ensure your services are accessible, ask more relevant questions such as "Do you need an interpreter? If yes, for what language?" For more ideas see Privacy Victoria, *Privacy in Diverse Victoria: Research report into attitudes towards privacy in diverse communities*, October 2002.
The collection of criminal records during recruitment poses particular risks.	Ensure that any law or policy requiring criminal record checks is able to demonstrate the relevance between the type of offending to be checked for and the employment position, and sets out when the check is to occur. For more advice, see Privacy Victoria, *Handling Criminal Records In The Public Sector*, Info Sheet 03.09, April 2009
For more ideas on risks and mitigation strategies associated with this Principle, see Privacy Victoria, *Guidelines to the Information Privacy Principles*, September 2006.	

Collection of unique identifiers (IPP 7.2 and 7.4) – Part 3 of the Template PIA report

COMMON RISKS TO CONSIDER	IDEAS FOR MITIGATION STRATEGIES
The risk of non-compliance with this principle if service provision is made conditional on the supply of a unique identifier.	Check carefully what personal information will be collected as part of the project. You can only demand a person's driver's licence number if you have specific legal authority to collect the number, or if your service depends on their demonstrated eligibility to drive. Even then, it may be enough to simply record that a current driver's licence has been sighted.
The risk of non-compliance with this principle if you plan to adopt an existing unique identifier as your own.	Check carefully how client records will be classified, labelled or stored as part of the project. You can only use another organisation's unique identifier for your own purposes in very limited circumstances, or with the person's consent. If your classification system will require uniformity (i.e. all clients to be numbered using the same system), then relying on consent will not be feasible.

Collection of unique identifiers (IPP 7.2 and 7.4) – CONTINUED

COMMON RISKS TO CONSIDER	IDEAS FOR MITIGATION STRATEGIES
The risk that a 'consent' to collect unique identifiers will not be valid.	Check the process by which you plan to seek consent. Ensure the consent will be truly voluntary (i.e. there will be no repercussions for individuals who refuse their consent), informed, specific, current and given by a person with the capacity to give or refuse their consent. If written consent cannot practicably be obtained, verbal consent should be recorded contemporaneously. For more advice about consent and capacity, see Privacy Victoria, *Guidelines to the Information Privacy Principles*, September 2006, under 'Key Concepts'.

For more ideas on risks and mitigation strategies associated with this Principle, see Privacy Victoria, *Guidelines to the Information Privacy Principles*, September 2006.

Use and Disclosure (IPP 2) – Part 3 of the Template PIA report

COMMON RISKS TO CONSIDER	IDEAS FOR MITIGATION STRATEGIES
The risk your use or disclosure of personal information is unlawful.	Seek legal advice to check that you have the lawful authority to operate this project. Be extra diligent in this regard if your project involves more than one organisation; you may not have the legal authority to use or disclose personal information on behalf of another organisation.
The risk that a use or disclosure 'compelled or permitted by or under a statute or the common law' is not compatible with the Charter of Human Rights and Responsibilities.	Seek legal advice to check that you have the lawful authority to use or disclose personal information because of another law; and that that law is compatible with the right to privacy in the Charter of Human Rights and Responsibilities.
The risk of legal non-compliance if the purpose for which you wish to use or disclose health information or sensitive information is not directly related to the primary purpose of collection.	Seek legal advice to check whether your proposed use or disclosure of health information or sensitive information will be considered directly related to the primary purpose of collection. If it is not, put in place a mechanism to seek the person's consent, or check if one of the other exemptions applies. Remember that for health information, the applicable rule is HPP 2, not IPP 2; there are some differences in the exemptions.
The risk of legal non-compliance if the purpose for which you wish to use or disclose other types of personal information is not related to the primary purpose of collection.	Seek legal advice to check whether your proposed use or disclosure will be considered related to the primary purpose of collection. If it is not, put in place a mechanism to seek the person's consent, or check if one of the other exemptions applies.
The risk of legal non-compliance if the individual would not reasonably expect you to use or disclose the information for the proposed purpose.	Ensure you have included all foreseen routine uses and disclosures in an appropriate privacy notice.

Use and Disclosure (IPP 2) – CONTINUED

COMMON RISKS TO CONSIDER	IDEAS FOR MITIGATION STRATEGIES
The risk of privacy complaints if people are surprised or upset by the secondary use or disclosure.	Use stakeholder consultation to test community expectations about your proposed uses and disclosures.
The risk of privacy complaints if the purpose of the secondary use or disclosure is not justifiable.	Where possible, make secondary uses and disclosures voluntary, i.e. seek consent first.
Projects involving the use of existing personal data for new purposes pose a particular risk.	Carefully check your project; your new purpose will either need to be directly related to the original purpose of collection, or consent obtained, or another exemption applied.
Data-sharing and data-matching pose particular privacy risks.	Carefully check your project if it involves data-sharing or data-matching across different business units or organisations. In your PIA Report, describe how the project will link or cross-reference separate databases. Explain why the data-matching needs to occur, and the effect on the project if the data-matching was not possible. Each participating organisation will need to have lawful authority to collect and/or disclose the information. Each piece of data to be collected will need to be necessary, fair, lawful and not unreasonably intrusive. Personal information can only be disclosed with consent, if specifically authorised under law, if directly related to the original purpose of collection, or if another public interest exemption applies. The data-matching program must also be transparent and fair. Individuals should be given prior notice of the fact and details of the proposed arrangement. If there may be negative repercussions for individuals, they should be given an opportunity to question the manner in which data has been processed to arrive at the adverse decision. Also observe the rules in the *Protective Security Manual*, which requires that classified data (including all personal information) can only be handed to another organisation if the other entity observes the same classification rules. (The *Protective Security Manual* is produced by the Commonwealth Government, but the Victorian Government has committed to protecting information in accordance with the Manual; see the Victorian Government *Framework for the Management and Protection of Security Classified Information*, 2008.)
The risk that authorising legislation will not be compatible with the Charter of Human Rights and Responsibilities.	If a legislative amendment is deemed necessary to provide the necessary lawful authority, or to revise a statutory prohibition, for the proposed use or disclosure, seek legal advice to ensure that the new law will be compatible with the right to privacy in the Charter of Human Rights and Responsibilities.
The risk that authorising legislation will not prevent future function creep.	Ensure new legislation is targeted and limited to the project at hand, and does not allow open-ended other collections, uses or disclosures.

Use and Disclosure (IPP 2) – CONTINUED

COMMON RISKS TO CONSIDER	IDEAS FOR MITIGATION STRATEGIES
The risk that of privacy complaints if people do not realise or remember that they have failed to 'opt out' of a voluntary secondary use or disclosure.	For voluntary secondary uses and disclosures, ensure the mechanism is 'opt in' rather than 'opt out'. Opt out systems may not be considered to constitute valid consent. Ensure the voluntary nature of the choice is clearly communicated in the privacy notice, including to people of a Non English Speaking Background or who may have limited capacity.
The risk that 'consent' to a secondary use or disclosure will not be valid.	Check the process by which you plan to seek consent. Ensure the consent will be truly voluntary (i.e. there will be no repercussions for individuals who refuse their consent), informed, specific, current and given by a person with the capacity to give or refuse their consent. If written consent cannot practicably be obtained, verbal consent should be recorded contemporaneously. For more advice about consent and capacity, see Privacy Victoria, *Guidelines to the Information Privacy Principles*, September 2006, under 'Key Concepts'.
The risk of legal non-compliance if a refusal of consent, or conditional consent, is not followed.	When relying on consent to authorise a secondary use or disclosure, ensure there is a workable mechanism by which the wishes of a person who refuses consent, or provides conditional consent, are recorded and acted upon promptly. Conditional consent may involve for example suppression of their identifying information or address details in your database, or de-identification before the results of a research project are disseminated.
Non-compliance with other legislation.	Check that any proposed disclosures will not breach secrecy provisions or other restrictions in your own legislation.
Non-compliance with other obligations.	Check that any proposed disclosures will not breach contractual or implied confidentiality undertakings.
The risk that de-identifying the information before disclosure does not prevent re-identification.	Removing client names is not de-identification if there are enough other details to allow the recipient to identify to whom the information refers, or match it to other information that would establish the person's identity.
The risk of legal non-compliance if ad-hoc uses or discloses are made of personal information which are not related to the primary purpose of collection.	Document in your PIA Report and in project policies what purposes for use or disclosure will and will not be considered to be related (or, in the case of health information and sensitive information, directly related) to the primary purpose of collection. Develop and communicate a procedure by which staff faced with a new or unusual request for use or disclosure can seek advice on whether this rule or an exemption applies. Ensure that decisions made in relation to ad-hoc requests are recorded; include the supporting reasons for the decision.

Use and Disclosure (IPP 2) – CONTINUED

COMMON RISKS TO CONSIDER	IDEAS FOR MITIGATION STRATEGIES
Possible use or disclosure for research or program evaluation purposes has not been considered up-front.	Seek consent up-front for research or program evaluation uses. Ensure the consent process is entirely voluntary, i.e. there will be no repercussions for individuals who refuse their consent. Seek the advice of your Human Research Ethics Committee (or equivalent) whether their approval would be needed for any research use or disclosure.
The publication of a public register online increases the risk of abuse of the information to locate and harm or threaten individuals.	Limit the online search facility to only provide for searches by property or by business name rather than by a person's name. For more advice, see Privacy Victoria, *Website Privacy – Guidelines for the Victorian Public Sector*, May 2004; and Privacy Victoria, *Public Registers and Privacy – guidance for the Victorian Public Sector*, August 2004.
The publication of a public register online increases the risk of bulk acquisition of personal information for purposes such as direct marketing, or data-matching for profiling purposes.	Limit access to the register to 'read only'; do not allow a download or printing of the register in bulk. For more advice, see Privacy Victoria, *Website Privacy – Guidelines for the Victorian Public Sector*, May 2004; and Privacy Victoria, *Public Registers and Privacy – guidance for the Victorian Public Sector*, August 2004.
The publication of a public register online increases the risk of bulk acquisition of personal information which then becomes out of date.	Make sure that, as far as reasonably practicable, individuals have notice of the bulk release and of their right to seek correction of data.
For more ideas on risks and mitigation strategies associated with this Principle, see Privacy Victoria, *Guidelines to the Information Privacy Principles*, September 2006.	

Use and Disclosure of unique identifiers (IPP 7.1 and 7.3) – Part 3 of the Template PIA report

COMMON RISKS TO CONSIDER	IDEAS FOR MITIGATION STRATEGIES
Unique identifiers (e.g. a driver's licence or passport number) can be used to track, link and match records about a person across different organisations, and thus build up a profile of that person. This also increases the risk of identity theft and fraud.	Develop your own client numbering system rather than adopting another agency's system. A multiplicity of identifiers presents a more robust system of protection against identity theft and fraud.
Single Sign-On (SSO) could be privacy invasive if unique identifiers are used.	Avoid using unique identifiers for SSO projects.
Data-matching using unique identifiers poses particular risks.	In your PIA Report, describe how the project will use unique identifiers to link or cross-reference separate databases. Explain why the data-matching needs to occur, and the effect on the project if unique identifiers could not be used.
For more ideas on risks and mitigation strategies associated with this Principle, see Privacy Victoria, *Guidelines to the Information Privacy Principles*, September 2006.	

Transborder data flows (IPP 9) – Part 3 of the Template PIA report

COMMON RISKS TO CONSIDER	IDEAS FOR MITIGATION STRATEGIES
The risk of transferring personal information out of Victoria in breach of this principle.	If you need to transfer personal information to someone outside Victoria, consider whether it is practicable to seek consent to the transfer.
The risk that 'consent' to a transborder transfer will not be valid.	Check the process by which you plan to seek consent. Ensure the consent will be truly voluntary (i.e. there will be no repercussions for individuals who refuse their consent), informed, specific, current and given by a person with the capacity to give or refuse their consent. If written consent cannot practicably be obtained, verbal consent should be recorded contemporaneously. For more advice about consent and capacity, see Privacy Victoria, *Guidelines to the Information Privacy Principles*, September 2006, under 'Key Concepts'.
The risk of transferring personal information out of Victoria without appropriate safeguards.	You will probably not be in a position to judge whether the recipient organisation is bound by a privacy law or binding scheme that is substantially similar to the *Information Privacy Act*. Ensure you have a scheme or contract with appropriate clauses to permit such transfers. For more advice, see Privacy Victoria, *Model Terms for Transborder Data Flows of Personal Information*, June 2006.
Extranets proposed as an access solution for a multi-party project may expose your organisation's data via any weak links in the architecture.	Thorough examination of proposed data flows and security protections, 'from cradle to grave', is particularly important for projects involving transborder data flows.
For more ideas on risks and mitigation strategies associated with this Principle, see Privacy Victoria, *Guidelines to the Information Privacy Principles*, September 2006.	

Data Quality (IPP 3) – Part 3 of the Template PIA report

COMMON RISKS TO CONSIDER	IDEAS FOR MITIGATION STRATEGIES
Failing to implement basic records management standards.	Ensure your records management complies with the Australian and international standard for records management, AS ISO 15489, available from www.standards.com.au The standard covers processes and controls to ensure the integrity of a record remains intact throughout its life cycle. This is relevant to both the Data Quality and Data Security privacy principles.
Migrating paper records to a digital or online format by re-keying data increases the risk of introducing inaccuracies.	Ensure a process of quality control to minimise errors or unauthorised modifications.

Data Quality (IPP 3) – CONTINUED

COMMON RISKS TO CONSIDER	IDEAS FOR MITIGATION STRATEGIES
Inaccurate data can increase the risk of unauthorised disclosure.	Double-check that you have up to date details like fax numbers and mailing addresses before transferring or disclosing personal information.
Automated decision-making can lead to unfair adverse outcomes for an individual.	Ensure particular controls are implemented when designing a project to involve automated decision-making. See Australian Government Information Management Office, *Automated Assistance in Administrative Decision-Making - Better Practice Guide*, February 2007.
The risk of poor quality data leading to poor or inaccurate decisions.	Establish procedures to determine when and how often personal information should be reviewed and/or updated. Check the reliability of equipment used to collect, process or test information or bodily samples. Ensure the project will include periodic checks of the accuracy and reliability of equipment, and human data processing.
Updating personal information without creating and maintaining audit trails of the updates increases the risk of unauthorised modification and poor data quality.	When data is to be updated or amended, ensure records are kept of the date and source of the last update, and ideally of every update.
Routine disclosures using static media (e.g. CDs/DVDs) can quickly lead to poor data quality for the recipient, as the data will age appreciably in a short time.	Caution should always be exercised when engaging in data-matching or data-cleansing, that the data is not already out of date.
Failing to update personal information that has been disclosed in the past can lead to poor data quality for the recipient.	Ensure there will be a procedure to notify routine recipients of your data, including contracted service providers, of subsequent updates.
Failing to update personal information held by contracted service providers can lead to poor data quality.	Ensure your contract includes provisions covering how correction requests are to be handled, and who is responsible for routine updates to the data. Consider which organisation will have the most current data, and how it can be made readily available.
Internet search engines such as Google retain cached data, even if it has been removed from a website consciously and immediately.	If personal information published online (e.g. in a public register) requires deletion, de-identification or amendment in the name of data quality, then it is not a simple matter to erase the 'incorrect' data from all search engines. They will need to be contacted to remove the data from their cache.
For more ideas on risks and mitigation strategies associated with this Principle, see Privacy Victoria, *Guidelines to the Information Privacy Principles*, September 2006.	

Data Security (IPP 4.1) – Part 3 of the Template PIA report

COMMON RISKS TO CONSIDER	IDEAS FOR MITIGATION STRATEGIES
Failing to implement basic information security standards.	Ensure your data security strategy complies with ISO 27001, *Information technology – Security techniques – Information security management systems – Requirements*, available from www.standards.com.au
Failing to implement basic records management standards.	Ensure your records management complies with the Australian and international standard for records management, AS ISO 15489, available from www.standards.com.au The standard covers processes and controls to ensure the integrity of a record remains intact throughout its life cycle. This is relevant to both the Data Quality and Data Security privacy principles.
Leaving weak spots in your data security across the range of data flows.	Examine your data flows diagram/s carefully, to see if there are any weak spots which require further data security measures.
Failing to implement a higher degree of security to protect sensitive information, health information, or personal information that could enable identity fraud if it were obtained without authority.	Ensure your data security strategy is appropriate to the type of data being stored. For more advice, see Privacy Victoria, *Guidelines to the Information Privacy Principles*, September 2006, under 'Data Security'.
Failing to recognise the high-risk nature of the data being stored.	Some types of personal information should attract the highest levels of security. For example, digitised signatures, photographs and other biometric information such as fingerprints or DNA, cannot simply be re-issued if they have been compromised through a data security breach.
Failing to include contracted service providers in your data security strategy. This is of particular concern if the contracted service provider is outside Victoria.	Ensure your contracted service providers are bound by the contract to comply with the IPPs. Ensure the contract also outlines more specific requirements relating to data security for your project.
Failing to limit access to data can increase the risk of misuse or unauthorised disclosure.	Develop robust access control protocols which limit access on a 'need to know' basis. Users should only have access to that portion of data they need to carry out their legitimate functions. Access control requires role definition to a suitably granular level. Otherwise, there may simply be 'standard users' and far too many 'power users'. Supervisors and managers do not necessarily need access to all the information accessible by their subordinates. Ensure the protocol also outlines who has the authority to assign, change or revoke access privileges.
Failing to limit edit-access to data can increase the risk of misuse or unauthorised amendment.	Develop access control protocols which cover who has the authority and ability to add, amend or delete data.

Data Security (IPP 4.1) – CONTINUED

COMMON RISKS TO CONSIDER	IDEAS FOR MITIGATION STRATEGIES
Failing to enforce access controls can increase the risk of misuse or unauthorised disclosure.	Ensure access controls are updated constantly and quickly, to accommodate departing staff, changes in roles, and the expiry of contractors' terms.
Failing to monitor access to data can increase the risk of misuse or unauthorised disclosure.	Ensure there is an audit system to log, by time and user ID, any edits to data (adding, amending or deleting data), and even any read-only access. Ensure employees are given notice of this logging, both for their own sake and in order to deter misuse.
The risk of external breaches of data security.	Consider conducting a threat and risk assessment of your database and network security, and possibly include an ethical hacking exercise.
Building access controls can involve inadvertent disclosure of personal information.	Ensure procedures for sign-in or registration don't unnecessarily reveal information about previous registrants or visitors to your premises.
Offices open to the public can pose a risk of unauthorised access to personal information.	Implement physical security measures such as preventing public access to areas where personal information is stored or used. Create separate meeting rooms in which no information is stored, and confidential discussions can take place.
Co-located offices and shared workstations can pose a risk of unauthorised access to personal information.	Implement a 'clean desk' policy, and provide a lockable filing cabinet for each user of a workstation. Where possible, limit staff access to floors or discrete areas, such as a room housing network servers or a file compactus, to those with appropriate permissions.
Devices in shared work areas, or portable devices, risk inappropriate access.	Implement password-protected automatic screensavers to come on after a short period of computer inactivity.
Allowing the use of portable storage devices (e.g. USB sticks) in the workplace can increase the risk of unauthorised disclosure or accidental loss of personal information.	Control the use of portable storage devices through carefully considered policies and technical controls. See also the recommendations in Privacy Victoria, *Use of Portable Storage Devices*, January 2009.
Using regular post to send personal information can increase the risk of unauthorised disclosure.	Use registered post to send health information, sensitive information, or any other personal information that could cause embarrassment, loss or hurt to the person, including through identity fraud, if it were received by someone else.
Posting personal information poses particular data security risks.	The use of window envelopes can avoid mixing up labeled envelopes and their intended contents for bulk mail-outs. Ensure that no information, beyond that needed for correct addressing, is included on the outside of an envelope, or is visible accidentally through the envelope window. For example, it should not be obvious without opening the envelope that the contents are a parking fine, the outcome of a job application, or health information.

Data Security (IPP 4.1) – CONTINUED

COMMON RISKS TO CONSIDER	IDEAS FOR MITIGATION STRATEGIES
Faxing personal information carries particular data security risks.	Ensure that if sending personal information by fax is necessary for your project, that staff are aware of the need to check carefully the fax number before sending, and to call ahead to ensure the intended recipient is on hand to collect the pages. Likewise if it is necessary for your project to receive personal information by fax, position your office fax machine so visitors or staff from other areas can't read the documents on it or near it.
Emailing poses particular data security risks during transmission of data.	Establish what personal information must be sent by email, and consider encryption, particularly for health information, sensitive information, or any other personal information that could cause embarrassment, loss or hurt to the person, including through identity fraud, if it were received by someone else.
Online transactions pose particular data security risks during transmission of data.	SSL (Secure Sockets Layer) encryption should always be used for online transactions. Also consider using EV (Enhanced Validation), which demonstrates that security is taken seriously. See also Privacy Victoria, *Website Privacy – Guidelines for the Victorian Public Sector*, May 2004, and Victorian Auditor-General, *Managing Internet Security: Good Practice Guide*, June 2004.
Providing online log-in access to client records raises the risk of automated scams.	Use CAPTCHA technology to differentiate between human and computer users of your site.
Entering information online or over the telephone poses risks for people using shared or public facilities.	Test your systems thoroughly to ensure subsequent users of a telephone or computer terminal cannot find out your client's data by using a 'last number recall' or 'back / refresh browser' function.
Allowing remote access to data poses particular data security risks.	Ensure that any remote access to your data, whether by staff or clients, is to encrypted data, or is unencrypted data which travels only via encrypted transmission. Also consider two-factor authentication rather than just username and password, and build-in a 'time out' limit on access.
Data-matching with other organisations carries particular data security risks.	Information classification assists in analysing the risk associated with data-matching, particularly by observing the rules contained in the *Protective Security Manual* (PSM), supported by the Information Security Manual, formerly known as ACSI33. The key consideration of the PSM is that classified data (including all personal information) can only be handed to another organisation if the other entity observes the same classification rules. Any media used to store the classified material automatically inherits that classification.

Data Security (IPP 4.1) – CONTINUED

COMMON RISKS TO CONSIDER	IDEAS FOR MITIGATION STRATEGIES
Testing and training environments may expose personal information to risk.	Ensure your project will use only dummy data in testing and training environments.
The risk of ignoring personal information held in backup tapes.	Ensure your data security measures apply equally to records made as backups.
The risk of ignoring the privacy of deceased individuals.	Information about the deceased may reveal information about the living. Ensure your data security measures apply equally to records containing information about the deceased. (Note: Under the Victorian *Health Records Act*, health information is further protected for 30 years after death).
Staff who are unaware of their obligations pose data security risks.	Ensure your project will include staff training and plain language policies to supplement your other data security measures.
For more ideas on risks and mitigation strategies associated with this Principle, see Privacy Victoria, *Guidelines to the Information Privacy Principles*, September 2006.	

Data Disposal (IPP 4.2) – Part 3 of the Template PIA report

COMMON RISKS TO CONSIDER	IDEAS FOR MITIGATION STRATEGIES
Keeping data longer than it is required increases the risk of a data security breach or unauthorised use or disclosure.	Check whether you have an existing Records Authority from the Victorian Public Records Office (PROV) that will cover data collected for the project; if not, seek advice from PROV on the appropriate disposal action. For transactional data, aim to destroy the data as soon as the transaction is complete. Ensure personal information is disposed of promptly once the minimum retention period specified in the Authority has expired, unless you have a legitimate purpose for retaining the information for longer. For health service providers, also see the *Health Records Act 2001 (Vic)*.
Not knowing how old your records are increases the risk of a data security breach or unauthorised use or disclosure.	Design your database to include a facility to flag records for review or deletion at the expiry of the minimum retention period.
The disposal of assets poses privacy risks.	Ensure hard disks are entirely wiped or encrypted before disposing of computers.
The disposal of paper files poses privacy risks.	Use a shredder or secure disposal bins for disposing of paper records.
For more ideas on risks and mitigation strategies associated with this Principle, see Privacy Victoria, *Guidelines to the Information Privacy Principles*, September 2006.	

Access (IPP 6.1 and FOI Act) – Part 3 of the Template PIA report

COMMON RISKS TO CONSIDER	IDEAS FOR MITIGATION STRATEGIES
Remember that for much of the Victorian public sector, access is covered by the FOI Act.	
Not allowing people to easily access their personal information can increase the risk of poor quality data.	Facilitate straight-forward access and correction procedures. Consider providing individuals with routine access to their personal information, e.g. through online access to their accounts. (Remember that this needs to be weighed up against IPP 4, the Data Security principle.)
Access may be hampered if the data is held by contracted service providers.	Contracted service provisions may not be covered by the FOI Act. Ensure your contract includes provisions covering how access requests are to be handled. Consider which organisation will have the current data, and how it can be made readily available. Specify whether access is to be mediated by your organisation, or handled directly by the contracted service provider.
For more ideas on risks and mitigation strategies associated with this Principle, see Privacy Victoria, *Guidelines to the Information Privacy Principles*, September 2006.	

Correction (IPP 6.5 and FOI Act) – Part 3 of the Template PIA report

COMMON RISKS TO CONSIDER	IDEAS FOR MITIGATION STRATEGIES
Remember that for much of the Victorian public sector, correction is covered by the FOI Act.	
Poorly managed correction requests can frustrate people.	Ensure there is a clearly defined process by which an individual may discuss or dispute the accuracy of their personal information you hold. Recognise that different procedures will be appropriate for simple versus complex requests.
Poorly managed correction requests can lead to poor data quality.	Ensure you have a policy which sets out who in your organisation can action routine or simple correction requests (e.g. a client's change of address), and who can determine more complex requests (e.g. a client disputes your decision on their eligibility for services). Ensure there a record kept of correction requests, and of your subsequent decision whether or not to correct.
Correction may be hampered if the data is held by contracted service providers.	Contracted service provisions may not be covered by the FOI Act. Ensure your contract includes provisions covering how correction requests are to be handled. Consider which organisation will have the current data, and how any corrections will be communicated to the other organisation. Specify whether correction requests are to be mediated by your organisation, or handled directly by the contracted service provider.
Failing to correct personal information that has been disclosed in the past can lead to poor data quality for the recipient.	Ensure there will be a procedure to notify routine recipients of your data of subsequent corrections to the data.
For more ideas on risks and mitigation strategies associated with this Principle, see Privacy Victoria, *Guidelines to the Information Privacy Principles*, September 2006.	

Bodily privacy – Part 4 of the Template PIA report

COMMON RISKS TO CONSIDER	IDEAS FOR MITIGATION STRATEGIES
The risk that an intrusion into bodily privacy is not compatible with the Charter of Human Rights and Responsibilities.	Seek legal advice to check that you have the lawful authority to touch another person's person or belongings; and that that law is compatible with the right to privacy in the Charter of Human Rights and Responsibilities.
An unnecessary search of a person's body or belongings could breach a person's right to privacy.	Ensure any intrusion into bodily privacy is necessary, a proportionate response to an identifiable and significant risk, and is subject to appropriate oversight and accountability mechanisms.
An unduly intrusive search of a person's body or belongings could breach a person's right to privacy.	Ensure the public benefit in conducting searches outweighs the public interest in privacy. The risk posed by not searching needs to be significant, and the response needs to be proportionate to that risk.
An arbitrary search of a person's body or belongings could breach a person's right to privacy.	Ensure there is a clearly communicated policy on search procedure available at the site of the search. Include the policy in your PIA Report.
Being searched in public can be embarrassing for many people, and particularly traumatic for some.	Provide separate, individually screened areas for people whose person or belongings need to be searched. Be aware of gender and cultural sensitivities, and have appropriately trained staff.
The risk of community backlash if special sensitivities are not considered.	Consider community expectations if you will be touching children, people with a disability, or people with particular religious or cultural beliefs.
Searches and screening can reveal personal information not relevant to your needs.	Ensure that any personal information revealed during a search or screen that is not relevant to your purposes is not recorded, or is erased immediately, or cannot be linked to that person's identity.
Records obtained from searches or screening pose data security risks.	Where records do need to be kept, ensure you have appropriate data security measures to protect the data, including access controls, audit mechanisms and encryption.
The risk of privacy complaints if the program is not transparent.	Ensure there is appropriate notice to people about the program.

Territorial privacy – Part 4 of the Template PIA report

COMMON RISKS TO CONSIDER	IDEAS FOR MITIGATION STRATEGIES
The risk that an intrusion into territorial privacy is not compatible with the Charter of Human Rights and Responsibilities.	Seek legal advice to check that you have the lawful authority to enter another person's home or private space; and that that law is compatible with the right to privacy in the Charter of Human Rights and Responsibilities.
An unnecessary intrusion into a person's home or other private space could breach a person's right to privacy.	Ensure any intrusion into territorial privacy is necessary, a proportionate response to an identifiable and significant risk, and is subject to appropriate oversight and accountability mechanisms.
A failure to provide appropriate private space could breach a person's right to privacy.	Consider whether your premises need private spaces such as change-rooms or breast-feeding facilities.
Searches and surveillance can reveal personal information not relevant to your needs.	Ensure that any personal information revealed during a search or surveillance that is not relevant to your purposes is not recorded, or is erased immediately, or cannot be linked to that person's identity. Ensure you are complying with the *Surveillance Devices Act*.
Records obtained from searches and surveillance pose data security risks.	Where records do need to be kept, ensure you have appropriate data security measures to protect the data, including access controls, audit mechanisms and encryption.
The risk of privacy complaints if the program is not transparent.	Ensure there is appropriate notice to people about the program.

Locational privacy – Part 4 of the Template PIA report

COMMON RISKS TO CONSIDER	IDEAS FOR MITIGATION STRATEGIES
The risk that an intrusion into locational privacy is not compatible with the Charter of Human Rights and Responsibilities.	Seek legal advice to check that you have the lawful authority to track or monitor another person's whereabouts; and that that law is compatible with the right to privacy in the Charter of Human Rights and Responsibilities.
Unnecessary tracking of a person's whereabouts could breach a person's right to privacy.	Ensure any intrusion into locational privacy is necessary, a proportionate response to an identifiable and significant risk, and is subject to appropriate oversight and accountability mechanisms. Ensure you are complying with the *Surveillance Devices Act*.
Location-tracking can reveal personal information not relevant to your needs.	Ensure that any personal information revealed during location-tracking that is not relevant to your purposes is not recorded, or is erased immediately, or cannot be linked to that person's identity. Check whether the technology can be switched off; for example, whether GPS tracking of fleet vehicles is appropriate outside of work hours.

Locational privacy – CONTINUED

COMMON RISKS TO CONSIDER	IDEAS FOR MITIGATION STRATEGIES
Records obtained from location-tracking pose data security risks.	Where records do need to be kept, ensure you have appropriate data security measures to protect the data, including access controls, audit mechanisms and encryption.
The risk of privacy complaints if the program is not transparent.	Ensure there is appropriate notice to people about the program.
For more ideas on risks and mitigation strategies associated with this Principle, see Privacy Victoria, *Guidelines to the Information Privacy Principles*, September 2006.	

Communications privacy – Part 4 of the Template PIA report

COMMON RISKS TO CONSIDER	IDEAS FOR MITIGATION STRATEGIES
The risk that an intrusion into communications privacy is not compatible with the Charter of Human Rights and Responsibilities.	Seek legal advice to check that you have the lawful authority to intercept or record another person's communications; and that that law is compatible with the right to privacy in the Charter of Human Rights and Responsibilities.
Conversations involving client personal information may be overheard.	Consider your building layout to ensure staff and clients can have private conversations where appropriate.
Non-compliance with other legislation.	Check that your project will comply with your own enabling legislation, and any other applicable legislation such as the *Surveillance Devices Act 1999* and the *Telecommunications (Interception) Act*.
Monitoring or recording communications can reveal personal information not relevant to your needs.	Ensure that any personal information revealed through monitoring or recording communications that is not relevant to your purposes is not recorded, or is erased immediately, or cannot be linked to that person's identity.
Records obtained from communications monitoring pose data security risks.	Where records do need to be kept, ensure you have appropriate data security measures to protect the data, including access controls, audit mechanisms and encryption. Records will be subject to the *Information Privacy Act*.
The risk of privacy complaints if the program is not transparent.	Ensure there is appropriate notice to people about the program.

Openness (IPP 5) – Part 5 of the Template PIA report

COMMON RISKS TO CONSIDER	IDEAS FOR MITIGATION STRATEGIES
Privacy policies need to be appropriate.	Check whether your organisation already has a privacy policy covering your collection and information handling practices. Consider whether it needs to be amended in light of this project, and/or whether the project should have its own privacy policy. Set regular dates to review and update the privacy policy.
Privacy policies need to be accessible.	Ensure the appropriate privacy policy is easily understandable and accessible on your website, and available in other formats on request. See also Privacy Victoria, *Website Privacy – Guidelines for the Victorian Public Sector*, May 2004.
Privacy policies need to be well communicated.	Establish a communications plan to explain to stakeholders and the public how personal information will be managed and protected as part of this project.
Online transactions can involve several entities.	Related privacy statements need to give the user enough background information for them to decide whether to proceed. Simply referring to one organisation's statement may not be sufficient. Ensure access is to the correct policy for each entity involved.

The privacy management function – Part 5 of the Template PIA report

COMMON RISKS TO CONSIDER	IDEAS FOR MITIGATION STRATEGIES
Failing to make contingency plans in relation to data loss.	Ensure your organisation has risk management procedures to recover personal information in the case of loss or damage. Consider risks including human error, theft, malicious attack, computer error, network security flaw and natural disaster.
Failing to respond pro-actively to privacy breaches.	Ensure you have procedures in place to identify and respond to data security breaches. This will include containment, evaluation, notification and mitigation / prevention. (See Privacy Victoria, *Responding to Privacy Breaches*, May 2008.) Document or refer to these procedures in your PIA Report. Ensure all personnel handling personal information for the project are aware of these procedures.
Unclear complaint procedures.	Ensure there are clear procedures and responsibilities assigned for handling complaints about privacy. Ensure all personnel handling personal information for the project are aware of the complaint process.

The privacy management function – CONTINUED

COMMON RISKS TO CONSIDER	IDEAS FOR MITIGATION STRATEGIES
Failure to learn from mistakes.	Ensure there is a mechanism by which privacy complaints will trigger a review of your project to see if further mitigation strategies are needed to improve privacy protection.
Staff who are unaware of their obligations pose data security risks.	Ensure your project will include staff training and plain language policies covering their obligations when handling personal information.

Accountability – Part 5 of the Template PIA report

COMMON RISKS TO CONSIDER	IDEAS FOR MITIGATION STRATEGIES
Lack of transparency about the privacy negatives and positives arising from the project.	Publish your PIA Report (or appropriate extracts) on your website. Provide a copy of your PIA Report to Privacy Victoria.
Lack of oversight of changes to the project.	Ensure you have an oversight committee or other independent person or body to: • promote and report on compliance • review any requests for amendments to the project, review any proposals for new uses or disclosures of the data, conduct or commission privacy audits, and investigate and resolve complaints.
PIAs can become out of date.	Privacy audits can assist by reviewing whether a project is meeting its objectives, whether anything about the project has changed, how personal information is actually being handled, and whether your original PIA's conclusions and recommendations remain valid. Establish a timetable in which to conduct regular reviews of your project. Ensure you review the effectiveness of data collection compared with its stated purpose; be prepared to stop any collection of personal information not serving a clear public purpose. Also consider that technologies may have since developed which enable more privacy-enhancing approaches to be taken.
Projects will not be needed forever.	Consider up-front whether the project should have a 'sunset clause', i.e. stop after a set period of time unless pro-actively reviewed and renewed. This should include disposal mechanisms.

The Information Privacy Principles are simply…

the right information,
to the right people,
for the right reason,
in the right way,
at the right time.

Office of the
Victorian Privacy
Commissioner

GPO Box 5057
Melbourne Victoria 3001
Australia
DX 210643 Melbourne

Level 11
10-16 Queen Street
Melbourne Victoria 3000
Australia

Local Call 1300 666 444
Local Fax 1300 666 445

www.privacy.vic.gov.au
enquiries@privacy.vic.gov.au