State Government Victoria
Department of Education & Training

Privacy Compliance Assistance Package

Guidelines to assist with privacy compliance in children's services

Children's services manage a wide range of personal and health information.

The purpose of this package is to assist children's services in developing a plan for complying with the privacy laws. The plan may be useful in identifying where current practices meet privacy compliance requirements, where the gaps are and what changes may be needed to improve practice.

Contents

Introduction

What is information privacy?

The term 'information privacy' refers to the protection of personal information, and the individual's right to control how information about them is handled.

Personal information is information about a person that identifies them, or could be used with other readily available information to identify them. It covers information in many forms.

Information privacy laws require us to only use personal information for the purposes for which it was collected and to protect that information against misuse. It also enables children's services to collect information they need to perform their activities and functions, as people are usually more willing to provide full and frank information if satisfied that it will be treated within a privacy framework.

This idea is not new – confidentiality and access have long been recognised and reflected as important values by the Department of Education and Training (DET) and children's services.

What are the Victorian Privacy Laws?

The Victorian laws are:

- *Information Privacy Act 2000* (IPA) covering non-health information – became law on 1 July 2002.
- *Health Records Act 2001* (hRA) covering health information – became law on 1 September 2002.

Managing compliance – responsibilities and obligations

This package is designed to assist children's services undertake a systematic review of all policies, procedures, IT systems and day-to-day practices to identify privacy risks.

To meet compliance requirements, children's services have a responsibility to review their day-to-day practices and core operational activity.

Flowchart for developing a privacy compliance plan

This flowchart shows a typical process that may be followed when developing a privacy compliance plan. The five stages are designed to assist you with assessing the level of compliance in your area and identifying what changes may be necessary to meet privacy requirements.

Stage 1 – Building on existing good practices $

Make a list of what has already been done in your service to comply with privacy legislation. Protection of privacy is not new and many areas already have well-established policies and protocols in place. Building upon these established policies and protocols will form the basis of your privacy compliance plan.

Stage 2 – Conduct a review $

A privacy review is a useful way of working out what sort of information your service collects, holds, uses and discloses.

Stage 3 – Identify problem areas $

Familiarise yourself with the privacy principles and how they might affect the way your service handles the flow of information. Compare your current practices with the privacy principles to highlight where there might be problems with compliance.

Stage 4 – Change practice to ensure compliance $

A plan will need to be developed to address any areas that do not comply with the privacy principles.

Stage 5 – Ongoing education and review

Your privacy plan will need to be regularly reviewed and monitored as new systems, policies and protocols are introduced. Training is essential to promote awareness of staff and volunteer responsibilities and obligations. A complaints handling mechanism ensures good practice and openness.

The following sections of this package refer to the five stages of the compliance plan mentioned above.

Stage 1 – Building on existing good practices

The privacy principles in the *Information Privacy Act 2000* and the *Health Records Act 2001* reflect ideas and standards that are familiar to many people working in children's services. A strong professional ethic already exists in relation to parent/guardian/child confidentiality and the protection of privacy. Meeting the Information Privacy Principles (IPP's) should not require a major overhaul of all existing procedures. It provides an opportunity to review procedures, protocols, policies and systems to ensure that they meet the requirements of the privacy laws.

Privacy in practice

The privacy laws protect personal and health information by setting standards on how it should be handled, from collection to disposal. The key messages in summary (some of which are qualified by prescribed exceptions, specifying circumstances when they do not apply) are:

- **only collect information you need for your specific purpose** (identify the primary purpose)
- **inform the person** – ensure they know why you need it and how you will handle it
- **only use the information for the purpose for which it was collected** or a directly related purpose which would be within the person's expectations
- **do not use, disclose or share the information for a different purpose without the person's consent** – unless you are specifically exempt under the Acts
- **provide the person with access to their information** on request
- **keep the information secure**, and dispose of it only when redundant, in accordance with statutory requirements.

Any effective review of privacy practice requires an understanding of the fundamental underpinnings of privacy laws. For further information about the Privacy Principles refer to Attachment 1.

In essence, privacy compliance means looking at existing practices and assessing whether changes need to occur to ensure privacy compliance. Privacy should be integrated into everyday practice and be seen as a core responsibility and not as an add on. Cultivate a privacy culture in your workplace, ensure staff are aware of their obligations and keep privacy on the agenda.

Identifying problem areas

1 Remember the fundamental rule

Information should only be used or disclosed for the purpose for which it was collected or a directly related purpose. The key exceptions are:

- if the person consents
- if the law authorises it
- one of the other exceptions listed in Information Privacy Principle 2 (for personal information) or health Privacy Principle 2 (for health information) applies.

2 Don't forget the impact of other legislation

Any other legislation containing specific rules for the handling of parent/guardian/child information (such as secrecy and confidentiality provisions, or powers to collect, or obligations to disclose) takes precedence over the *Information Privacy Act 2000* and the *Health Records Act 2001* only to the extent of any inconsistency.

3 Get advice if you need it

If you are unsure talk to Kindergarten Parents Victoria, Community Childcare Victoria, a Children's Services Advisor in your region[1], the Office of the Victorian Privacy Commissioner or the health Services Commissioner.

1. Contact details are at http: //www.education.vic.gov.au/licensedchildservices/

Stage 2 – Privacy compliance review

A privacy review is a useful way of working out what sort of information your service collects, holds, uses and discloses.

Applying the privacy principles to problems

The following points are useful when thinking about how to relate real examples or identified problems to the privacy principles as you conduct your privacy compliance review.

1 Does other legislation apply?

Is the information regulated by another Act? for example, the *Children's Services Act 1996, Adoption Act, Children, Youth and Families Act,* etc. If so, that other Act will regulate the information.

2 Is privacy relevant?

If the information in question is identifying or identifiable (i.e. it could be used with any other readily available information to identify an individual) then privacy principles apply.

If it definitely isn't identifying or identifiable, then privacy doesn't apply.

3 Which Act applies?

Section 56 of the *Children's Services Act 1996* provides that records are kept by children's services. The details of these records are prescribed in Part 3 of the *Children's Services Regulations 2009.* The *Health Records Act 2001* applies if the information in question is identifying/identifiable 'health information' – defined to include medical, psychiatric, psychological or disability information.

The *Information Privacy Act 2000* applies if the information in question is identifying/identifiable and is not health information (as defined above).

4 Which Principle applies?

Is the way in which the information has been or will be handled, about:

Collection? Use and disclosure? A request for access? Security? etc.

5 Does the principle allow the information to be handled in a particular way?

6 If not, does any exception to the principle allow it?

Check the detail – and keep in mind the most common exceptions are:

- consent (the person provides informed consent to it)
- the law requires or authorises it (e.g. another Act provides it must or can be done)
- an emergency requires it (serious and imminent threat of harm).

If in doubt, seek advice. (Refer to page 20 for information about who to contact)

Privacy compliance review

The following tables are designed to unpack the principles and enable you drill down to identify any compliance risks.

They provide some questions to consider when conducting a privacy compliance review. They will help you understand how the privacy principles may affect your particular children's service and highlight where you may have problems with compliance. Developing a good understanding of the basic underpinnings of privacy and the requirements of each principle will help you identify potential risk areas. The relevant policy guidelines will also assist in the risk identification process. An action plan will need to be developed to address any compliance problems.

Principles in summary	Question	Answer	Is there a privacy risk?	Action to address identified risk/ improve practice
Collection				
Health Privacy Principle (HPP1) Collect health information about an individual by lawful, fair and reasonable means necessary for an organisation's functions or activities and preferably from the individual concerned. Added requirement of also having the individual's consent or one of the other prescribed matters in hPP1. Before, or near, the time of collection, notify the individual of: • the organisation's contact details • the purpose of collection • the individual's right to access health information • usual disclosures • where the collection is required by law • the main consequence of not providing health information. When collecting health information from third parties, the subject of the information will need to be informed of the six points listed above. Information communicated in confidence from third parties can be collected. **Information Privacy Principle (IPP1)** Collect the personal information by lawful, fair and reasonable means necessary for an organisation's functions or activities and preferably collect it from the individual concerned. Before or near the time of collection notify the individual of: • the organisation's contact details • the purpose of collection • the individual's right to access personal information • usual disclosures • where the collection is required by law • the main consequences of not providing personal information. When collecting personal information from third parties, tell the individual whose personal information is collected of the six points listed above.	What information does your service collect?			
	Is any of this information personal information?			
	Is any of the information sensitive information?			
	Is any of the information health information?			
	how does your service collect this information?			
	What law authorises or requires the collection?			
	have you identified the purposes for which you collect personal and/or health information?			
	Are you confident that only necessary information is collected?			
	have you stopped collecting any information that you do not need and are not required to collect?			
	have you reviewed your collection practices to ensure they are fair, lawful and not unreasonably intrusive?			
	have you taken steps to ensure the parents/guardians are aware of why the information is collected and all the other details required of hPP1.4 and/or IPP1.3?			
	Do you have a collection statement which is included in brochures and given at the point of collection? Privacy Impact Assessments are available from www.education.vic.gov.au/privacy/			

* The Privacy Impact Assessment (PIA) suite of tools is designed to provide guidance when developing or reviewing processes/systems or policies that manage personal information and assists in identifying privacy related risks and appropriate remedies. The PIA Guidelines and template are available at www.education.vic.gov.au/privacy/

Principles in Summary	Question	Answer	Is there a privacy risk?	Action to address identified risk/ improve practice
Use and disclosure				
HPP2 Use or disclose health information: • for the primary purpose for which the information was collected • for a directly related secondary purpose an individual would reasonably expect • where individual consents • for law enforcement • for other prescribed exceptions. Where disclosure is for law enforcement make a written note of the disclosure. **IPP2** Use or disclosure of personal information: • for the primary purpose collected; • for a related secondary purpose an individual would reasonably expect; • where individual consents; • for law enforcement; or • for other prescribed exceptions. Where disclosure is for law enforcement make a written note of the disclosure.	how does your service usually use the information?			
	Is the information disclosed to anyone outside your service?			
	Was collection voluntary or mandatory?			
	Was the subject of the information informed, at the time of collection or since, that the information might be disclosed for particular reasons to the particular types of requesters?			
	Is the use or disclosure of information the primary purpose of collection?			
	If not, what are the secondary purposes and how do they relate to the primary purpose?			
	Do staff have access to, and have they been trained in, procedures for: • deciding whether to use or disclose information for secondary purposes without consent • recording requests, consents, decisions and other evidence of how and why the information has been managed.			
	Do you have protocols, memoranda of understanding, contracts or other agreements that address privacy to cover ongoing or routine disclosures to contractors, service partners and other organisations?			

Principles in Summary	Question	Answer	Is there a privacy risk?	Action to address identified risk/ improve practice
Data quality				
HPP3 Take reasonable steps to ensure that health information is accurate, complete, up-to-date and relevant to an organisation's functions. **IPP3** Take reasonable steps to ensure personal information is accurate, complete, up-to-date and relevant.	has your service introduced measures to check that personal information is accurate, complete and up-to-date when it comes to use or disclose it?			
	how is the accuracy and integrity of personal information ensured during electronic transmission?			
	Do you have procedures in place to ensure that appropriate changes and notations can be made to personal or health information at the individual's request?			
	Do you routinely prompt individuals to let you know if their details need to be updated because of a change in their personal circumstances?			
	Do you have procedures in place to ensure that details shared within the organisation, and/or with other organisations, are kept up-to-date as necessary?			

Principles in Summary	Question	Answer	Is there a privacy risk?	Action to address identified risk/ improve practice
Security* and retention				
HPP4 Take reasonable steps to protect health information held from misuse, loss, unauthorised access, modification or disclosure. A health service provider must retain health information for prescribed periods. A non-health service provider must retain it for as long as lawful purpose. Provisions dealing with retention in other Acts, such as the *Public Records Act*, and the *Children's Services Act 1996* apply to the public sector. **IPP4** Take reasonable steps to protect personal information held from misuse, loss, unauthorised access, modification or disclosure. Destroy or permanently de-identify information no longer required. Provisions dealing with retention in other Acts, such as the *Public Records Act* and the *Children's Services Act 1996*, apply to the public sector.	Where and how does your service store personal information? i.e. hard copy, electronically			
	Who has access to the personal information held by your service?			
	Who actually needs to have access?			
	What measures protect personal information from unauthorised access, modification, misuse, loss or disclosure? Do they need to be approved?			
	have your security procedures been reviewed following an assessment of the risk?			
	have staff/volunteers been trained in those procedures? Is it periodically refreshed?			
	Is compliance with the procedures monitored?			
	Are there procedures in place to routinely review information to identify what is no longer needed for any purpose and not required to be kept by law?			
	Is information that is no longer needed or required to be kept destroyed securely or de-identified?			
	Is information that is required by law to be kept, but is no longer used, stored separately and securely?			
	The following resources are available: *Portable Storage Device Guidelines* www.privacy.vic.gov.au *Recordkeeping Guidelines* www.prov.vic.gov.au			

* When considering security risks, review both physical risks (e.g. information left on whiteboards, files left unattended etc.) and also IT risks (e.g. confidential email sent to wrong person, inadequate password policy, appropriate guidelines for USB memory sticks etc.)

Principles in Summary	Question	Answer	Is there a privacy risk?	Action to address identified risk/ improve practice
Openness				
HPP5 Document clearly expressed policies on the management of health information. Make the policies available to anyone who asks. On request, take reasonable steps to let the enquirer know generally what sort of health information the organisation holds, for what purposes, and how it collects and manages that information. **IPP5** Document clearly expressed policies on management of personal information and steps individuals have to take to access personal information. Make policies available to anyone who asks. On request, take reasonable steps to let the enquirer know generally what sort of personal information is held, for what purposes, and how the organisation collects and manages that information.	What information does your service collect?			
Access and correction				
HPP6 Administrative or formal procedures for access to health information under the *Freedom of Information Act* will apply in the public sector. Where health information is held in the private sector, *Health Record Act* procedures will apply. Access to information collected after 1 July 2001 can be requestedl. If collected prior to 1 July 2001 at the minimum the individual is entitled only to a summary. If the individual is able to establish that their health information is not accurate, complete, and up-to-date, the organisation must take reasonable steps to correct the information. **IPP6** Administrative or formal procedures for access to personal information under the *Freedom of Information Act* will apply in the public sector. Provide the individual with access to personal information on request by the individual, except to the extent that prescribed exceptions apply. If an individual establishes that the information is not accurate, complete and up-to-date, the organisation must take reasonable steps to correct the information.	have you established access procedures to enable you to provide individuals with access to their information?			
	Do you advise people of their right to access information about them?			
	have you established good record-keeping procedures to assist meeting access requests?			

Principles in Summary	Question	Answer	Is there a privacy risk?	Action to address identified risk/ improve practice
Unique identifiers				
HPP7 Document clearly expressed policies on the 'may only assign' identifiers to individuals if it is necessary for an organisation to carry out any of its functions efficiently. A private sector organisation may not adopt as its own identifier of an individual an identifier that has been assigned to that person by a public sector organisation unless prescribed exceptions apply. **IPP7** A service may only assign unique identifiers to individuals if it is necessary to carry out functions efficiently. A service must not adopt as its own unique identifier of an individual a unique identifier of the individual that has been assigned by another organisation unless prescribed exceptions apply.	Does your service use identifiers?			
	Does your service share with other organisations any unique identifiers that it creates?			
	If so, does it warn those organisations that they must not adopt the identifier as their own identifier?			
Anonymity				
HPP8 Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation. **IPP8** Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation.	Would it be lawful and feasible to give individuals the option of conducting any transactions anonymously?			
Transborder data flows				
HPP9 May transfer health information about an individual to someone (other than the organisation or the individual) who is outside Victoria only if prescribed conditions apply. **IPP9** May transfer personal information about an individual to someone (other than the organisation or the individual) who is outside Victoria only if prescribed conditions apply.	Do you have protocols in place where necessary when information is transferred out of Victoria? Otherwise, do you have procedures that ensure the transfer is permitted by hPP9 or IPP9? Model terms for Transborder data flows. See www.privacy.vic.gov.au			

Principles in Summary	Question	Answer	Is there a privacy risk?	Action to address identified risk/ improve practice
Sensitive information				
IPP10 Must not collect sensitive information about an individual, such as their ethnicity or criminal record, unless prescribed exceptions apply.	Is the information you are collecting sensitive? If you are collecting sensitive information, is consent required? (Sensitive information defined by the *Information Privacy Act* includes information on racial or ethnic origin, political opinions, religious beliefs or affiliations, sexual preferences or practices, among others.)			
Transfer or closure of practice of health service provider				
HPP10 If the practice or business of a health service provider is to be transferred or closed, the provider must comply with a prescribed set of procedures and statutory guidelines, centering on notification to former clients and the public. **HPP11** Making information available to another health service provider In an individual requests a health service provider to make their information available to another provider, the former must comply with the request as soon as possible.				

Additional considerations

The following tables provide additional information which may be useful for children's services to consider when assessing compliance risks in the workplace. The Office of the Victorian Privacy Commissioner has developed extensive guidelines that illustrate in practical ways compliance issues in relation to the Information Privacy Principles.

Issue	Examples of good practice
Central data collection (may be de-identified/aggregate)	• Ensuring that notification and/or consent is obtained at entry into the service. • Ensuring that only minimum information necessary is collected.
Data matching	• Ensuring that protocols are established for information matching and sharing. *Guidelines for the Public Sector* are available at www.privacy.vic.gov.au that may be of use to children's services.
Security measures to support the protection of privacy	Ensuring that security measures to support the protection of privacy are in place including: • restricting physical and technological access to information to only those who need it • establishing audit trails to track who is accessing information.
Professional development training and privacy integrated as a core responsibility	• Ensuring that privacy training and awareness for staff and volunteers is an ongoing concern at your service. The Victorian Privacy Commissioner's Office runs regular training sessions. Details are available at www.privacy.vic.gov.au
Complaints	• ensure you have a complaints handling policy. Guidelines are available at www.privacy.vic.gov.au • ensure there are clear procedural guidelines for managing privacy complaints • ensure you have an appropriately senior person trained in complaint management that has authority to investigate and respond to matters

Direct service areas

Issue	Examples of good practice
Office practice	Ensuring that procedures and practice have been reviewed to minimise privacy compliance risks, e.g.: • ensuring that information collection practices in reception, open areas are privacy sensitive • ensuring that confidential information is not left on whiteboards that may be seen by unauthorised staff • ensuring that faxes are sent and received only by those they are intended for • establishing protocols for taking hard copies out of the office.
Tracking information through service system	Established processes for transmission of information outside of services, e.g.: • added protections such as encryptions or attachments when sending emails, particularly to web-based email accounts • restricted access to authorised users • protection against unauthorised disclosure, e.g. after-hours access • ensuring that information is secure at all times • ensure appropriate guidelines for portable storage devices like USB keys, PDAs, external hard drives, etc. • ensuring there are audit trails to show who has access to the information • signs above photocopiers and faxes advising that personal information must not be left there • security protection for laptops.
Security measures to support the protection of privacy	

Individuals

Issue	Examples of good practice
Workplace	• a clean desk policy • ensuring that filing cabinets are locked and secure • not displaying passwords on the side of computers • not leaving files unattended • not leaving personal information in whiteboards • ensuring unauthorised personal cannot enter restricted areas.
Staff or parent/guardian/child's information	• ensuring that when carrying hard or soft copies of personal information files they are in sealed satchels when outside the workplace • ensuring that sealed satchels containing personal information are always in your personal possession or locked away securely • not creating unnecessary duplicate files • destroying multiple copies of information • not discussing personal information with people who do not need to know that information.

Stage 3 – Identify problem areas

The next step is to analyse the answers to the privacy compliance review and consider best practice examples. This will assist in assessing your level of privacy compliance and identify any risk. you will need to familiarise yourself with the privacy principles to see how they might affect the way your area handles the flow of information. The tools available on the Office of the Victorian Privacy Commissioners website and elsewhere might be useful in assessing the risk.

A review might also reveal that some of the information that you collect may no longer be necessary or relevant to your purposes. It may also assist you in understanding how information flows throughout the organisation and may highlight which practices could be changed or which systems could be improved.

your review should have identified the key risk areas and provided the framework for action. For example, a review of forms used to collect parent/guardian/child's information might reveal that some of that information collected is not allowed under privacy laws. Similarly, a review of the workplace may reveal that personal information is displayed in whiteboards and is visible to the general public.

Consider best practice examples and how this can be replicated in your workplace.

Threshold questions

The following are some threshold questions that may be relevant to your circumstances (this list is not exhaustive):

- have you identified the purposes for which you collect personal and/or health information?
- Are you confident that only necessary information is collected?
- have you stopped collecting any information that you do not need and are not required to collect?
- Do your procedures/policies address notification requirements?
- Can you collect the information in an unidentified form? Are you confident that your service meets the use and disclosure standards set by the legislation?
- Do you have protocols, memoranda of understanding, contracts or other agreements that address privacy?
- What measures protect personal information from unauthorised access, modification, misuse, loss or disclosure? have you considered records management issues and privacy issues?
- have you actively encouraged your staff and volunteers to attend privacy training?

Stage 4 – Change practice to ensure compliance

The analysis in stage 3 will form the basis of your compliance plan, identifying those areas where current practice does not meet the requirements of the privacy legislation and will need to be changed, modified or replaced.

This might include:

- amendments to current practice or the development of new practices
- changes to the way information is collected, used or stored
- the redesign of forms
- changes in policy, protocols and procedures
- changes to existing IT systems or the adoption of new technologies
- training to ensure provisions reflected in policies are put into practice.

Ideally, the analysis should not limit itself to compliance issues but also look to advantages and risks of retaining, amending or developing new practices around the collection, use and disclosure, managing and transferring of personal and/or health information. For example, an analysis of the way data is collected may result in a simpler form, which may be easier to complete and saves time and resources.

To ensure that the privacy compliance plan results in actual changes in practices, clear delegations of responsibility will need to be established, as will strict timeframes for completion of the project.

Where to start – some hints and ideas

1 Look at how and where you record information

How do you record information?

- Is it on file?
- On a laptop computer?
- On unattached pieces of paper?
- In more than one place?
- Do you have duplicate records that are not all maintained as carefully as each other?

2 Look at how securely you store information

- Who else knows your computer password?
- Where do you keep the key to your filing cabinet?
- Do you leave parent/guardian/child's information on your desk when you are not there?
- Are you putting unprotected parent/guardian/child's information on shared computer drives that people not working with your parent/guardian/child can access?

Make sure that you can demonstrate, through your own practices, that you are taking reasonable steps to protect the parent/guardian/child's or staff information from misuse.

3 Look at who you transmit and share information with

- Why do you share this information? Is it necessary?
    - Who do you share information with?
    - Do your parent/guardians know?

Check that you have their consent, or the authority of law, to share it.

Stage 5 – Review, monitoring and education

Regular monitoring and review

Where a children's service must comply with privacy legislation it should not stop with just one review. To maintain best practice, compliance should be an ongoing process that becomes built in to everyday practice.

The following should continue to occur:

- review the inventory of personal and/or health information on a regular basis
- ensure new systems comply with privacy laws
- implement a general awareness campaign for all staff in relation to privacy issues
- ensure that your privacy policy is available to all staff.

Children's services need to demonstrate a systematic approach to ensuring that procedures are followed, that staff training has been adequate, and that we are learning from the outcomes of any complaints. A series of audits (see www.privacy.vic.gov.au) and feedback mechanisms should ensure that apparent failures to comply are addressed and security measures are regularly monitored.

Education

Incorporate privacy into wider management responsibilities

having staff who are trained in privacy not only shows our commitment to complying with the legislation, it also complements and supports management responsibilities for quality assurance, service improvement, risk management, service coordination, openness and accountability. By incorporating your responsibility to protect privacy with these other responsibilities – rather than keeping it as a separate activity – you are likely to expend less resources, yet see better outcomes in all areas. Regular training of existing and new staff ensures that privacy awareness and compliance is built into everyday practice.

Cultivate a privacy culture

Convey the commitment to protect privacy within your service. Staff and volunteers should know that, not only is this required by law, it is in accordance with your organisation's values. Discuss with staff and volunteers any compliance weaknesses and strengths in your area and identify ways to improve where necessary.

Have a complaints handling process

Be ready to deal with complaints. Under the privacy legislation an individual can complain to the Privacy Commissioner or the health Services Commissioner about any act or practice of an organisation that the person claims is an interference with his or her privacy.

Simple and well-promoted internal systems for individuals to seek access to their information, find out more about privacy policy, and make a complaint if they feel it necessary, show that you are prepared to be open and accountable.

Complaints can also highlight systemic issues in policy, procedures and practice and identify where we need to improve and how we can do better.

Training materials

The Office of the Victorian Privacy Commissioner runs free regular training sessions. The Commissioner's Office also has a suite of training materials that can be used by an organisation's in-house trainer. See www.privacy.vic.gov.au for details.

Who to contact for more information

Health Services Commissioner (HSC)

For general information about the *Health Records Act 2001* visit the hSC website www.health.vic.gov.au/hsc or phone 86015222

Office of the Victorian Privacy Commissioner

For general information about the *Information Privacy Act 2000* visit www.privacy.vic.gov.au or phone 8619 8719

Federal Privacy Commissioner

If your query is in relation to the operations of a Commonwealth-funded agency, the privacy of information collected and/or used within the Commonwealth Public Sector is primarily covered under the *Privacy Act 1988*. Department of Education and Early Childhood Development (DEECD) cannot provide formal advice in relation to this Act.

General information about the *Privacy Act 1988* is available from Federal Privacy Commissioner website at www.privacy.gov.au/

DEECD Licensed Children's Services Enquiry Line: 1300 307 415, for matters related to requirements of the *Children's Services Act 1996* and Regulations (not privacy advice).

Attachment 1 – Key privacy principles in summary

This table sets out a summary version of some key privacy principles from the two Victorian Acts, as published by the health Services Commissioner and the Victorian Privacy Commissioner respectively.

These do not set out the full set or form of the principles, and are intended for quick reference only. The principles in full can be found in the respective Acts.

HEALTH PRIVACY PRINCIPLES SUMMARY	INFORMATION PRIVACY PRINCIPLES SUMMARY
1 Collection Only collect health information if necessary for the performance of a function or activity and with consent (or if it falls within hPP1). Notify individuals about what you do with the information and that they can gain access to it.	**1 Collection** Collect only personal information that is necessary for performance of functions. Advise individuals that they can gain access to personal information.
2 Use and disclosure Only use or disclose health information for the primary purpose for which it was collected or a directly related secondary purpose the person would reasonably expect. Otherwise, you generally need consent.	**2 Use and disclosure** Use or disclose personal information only for the primary purpose for which it was collected or a secondary purpose the person would reasonably expect. Use for secondary purposes should have the consent of the person.
3 Data quality Take reasonable steps to ensure health information you hold is accurate, complete, up-to-date and relevant to the functions you perform.	**3 Data quality** Make sure personal information is accurate, complete and up-to-date.
4 Data security and retention Safeguard the health information you hold against misuse, loss, unauthorised access and modification. Only destroy or delete health information in accordance with hPP4.	**4 Data security** Take reasonable steps to protect personal information from misuse, loss, unauthorised access, modification and disclosure.
5 Openness Document clearly expressed policies on your management of health information and make this statement available to anyone who asks for it.	**5 Openness** Document clearly expressed policies on management of personal information and provide the policies to anyone who asks.
6 Access and correction Individuals have a right to seek access to health information held about them in the private sector, and to correct it if it is inaccurate, incomplete, misleading or not up-to-date.*	**6 Access and correction** Individuals have a right to seek access to their personal information and make corrections. Access and correction will be handled mostly under the *Victorian Freedom of Information Act.*
7 Identifiers Only assign a number to identify a person if the assignment is reasonably necessary to carry out your functions efficiently.	**7 Unique identifiers** A unique identifier is usually a number assigned to an individual in order to identify the person for the purposes of the organisation's operations. Tax File numbers and Driver's Licence numbers are examples. Unique identifiers can facilitate data matching. Data matching can diminish privacy. IPP7 limits the adoption and sharing of unique numbers.

* In the public sector individuals already have this right under Freedom of Information.

HEALTH PRIVACY PRINCIPLES SUMMARY	INFORMATION PRIVACY PRINCIPLES SUMMARY
8 Anonymity Give individuals the option of not identifying themselves when entering transactions with organisations where this is lawful and practicable.	**8 Anonymity** Give individuals the option of not identifying themselves when entering transactions with organisations where that would be lawful and feasible.
9 Transborder data flows Only transfer health information outside Victoria if the organisation receiving it is subject to laws substantially similar to the hPPs.	**9 Transborder data flows** Basically, if your personal information travels, your privacy protection should travel with it. Transfer of personal information outside Victoria is restricted. Personal information may be transferred only if the recipient protects privacy under standards similar to Victoria's IPPs.
10 Transfer/closure of practice of health service provider If you're a health service provider, and your business or practice is being sold, transferred or closed down without you continuing to provide services, you must give notice of the transfer or closure to past service users.	**10 Sensitive information** The law restricts collection of sensitive information such as an individual's racial or ethnic origin, political views, religious beliefs, sexual preferences, membership of groups or criminal record.
11 Making information available to another health service provider If you're a health service provider you must make health information relating to an individual available to another health service provider if requested by the individual.	

FOR INFORMATION AbOUT THE HEALTH RECORdS ACT	FOR INFORMATION AbOUT THE INFORMATION PRIVACY ACT
health Services Commissioner 30th Floor, 570 Bourke Street Melbourne Victoria 3000 Telephone: 1800 136 066 Website: www.health.vic.gov.au/hsc	Victorian Privacy Commissioner Level 11, 10–16 Queen Street Melbourne Victoria 3000 Telephone: 1300 666 444 Website: www.privacy.vic.gov.au

Attachment 2 – Privacy collection statement creator

The following format may be of assistance in drafting a privacy collection statement to be provided either orally, say as a standard script, or in writing on forms and letters. Additional notification can also be given using brochures, posters and counter signage. Children's services that interact frequently with members of the public may choose to automatically overprint a privacy statement as a footer on the service's's letterhead template.

The wording seeks to achieve a combination of ensuring the individual is reasonably aware of the matters listed at IPP1.3 and hPP1.3 and also to obtain consent (if applicable) for use and disclosure of personal information that may not be for the primary or secondary related and ordinarily expected purposes of the collection.

Changes to the wording should not be made without seeking advice that the amended wording meets the requirements of privacy laws.

SAMPLE TExT	MANdATORY/OPTIONAL
The [name of service] service collects personal information for the purposes of [describe purposes e.g. to provide a service or associated administrative purposes].	Mandatory.
The collection of this information is required by [name the legislation].	Mandatory, where applicable. For example, include if a specific section of an Act requires stated personal information to be collected.
Without this information [specify consequences, e.g. we are unable to process your application/provide you with the service sought].	Mandatory.
We may disclose your information to [describe type of organisations/bodies to whom information maybe disclosed to assist with the delivery of service described above].	Mandatory if disclosing – include if you know the types of organisations you are likely to disclose information to.
you are able to request access to the personal information that we hold about you, and to request that it be corrected. Please contact the service directly on [phone number].	Mandatory.


NEALS