YOUTH PARTNERSHIPS:

COORDINATING SERVICES TO HELP YOUNG PEOPLE STAY ON TRACK

PRIVACY PACKS FOR DEMONSTRATION SITES

Table of Contents

Summary

In September 2011, the Youth Partnerships Secretariat engaged Bainbridge Associates Pty Ltd to undertake a Privacy Impact Assessment (PIA) of the Youth Partnerships initiative.

The PIA was undertaken from September – December 2011 with a Workshop involving key stakeholders held on 8 December 2011. This allowed stakeholders an opportunity to provide feedback on the PIA's preliminary findings and proposed recommendations.

The PIA Report was finalised in January 2012 and established that the Youth Partnerships initiative was not sufficiently advanced for a comprehensive PIA to be to be completed. However, it was noted that practical steps can be taken to build a strong privacy foundation for the initiative.

In consultation with Bainbridge Associates Pty Ltd, the Youth Partnerships Secretariat has developed this document which includes:

- advice on how to approach privacy and information sharing;
- a set of privacy tenets to guide good practice;
- frequently asked questions on privacy and information sharing;
- a privacy management framework checklist; and
- the Youth Partnerships Privacy Impact Assessment report.

The Secretariat will further develop detailed privacy content which will be incorporated in the Youth Partnerships website. It will include detailed guidance for stakeholders and youth practitioners in relation to their privacy obligations, including discussion of common privacy issues and illustrative case studies as well as providing a home for generic privacy forms, policies and protocols.

Information Sharing

Providing more coordinated services to young people in a partnership context requires the sharing of information about specific young people between participating organisations and their staff members. In order to ensure that this is undertaken in a way that complies with all relevant legislative requirements and respects privacy, an appropriate framework for information sharing needs to be developed and documented.

Any information sharing needs to take account of the following information sharing principles[1] prior to implementation:

- Partnership organisations must act within the limits of relevant legislation (including confidentiality and privacy requirements) when sharing information;
- Clear governance arrangements to ensure that privacy is supported within each individual Youth Partnerships demonstration site;
- Open and accountable processes and procedures must provide support for information sharing;
- Information sharing must be consistent with applicable privacy principles;
- Information sharing procedures must account for the security and quality of personal information, including confidential information; and
- Information sharing must occur within an agreed context of information policies, procedures and practices, relevant legislation and privacy principles.

Documenting an information-sharing framework has the capacity to provide greater clarity, transparency and consistency for participants and stakeholders and should be developed as part of **Step Two – Structuring the Partnership**. It may include an information-sharing policy; a template MOU for information sharing; and/or model consent form(s).

Information Privacy

Information privacy is a necessary component of any information-sharing framework whenever personal information is involved. This is for two main reasons: on the one hand, privacy poses a significant risk to information sharing if it is not managed effectively; on the other, good privacy practice is able to strengthen and enhance information sharing.

Privacy is regularly identified as a potential or actual impediment to the more coordinated delivery of youth services, particularly in terms of sharing personal information. While it is commonplace to hear that privacy poses an impediment to improved information sharing, this view must be challenged.

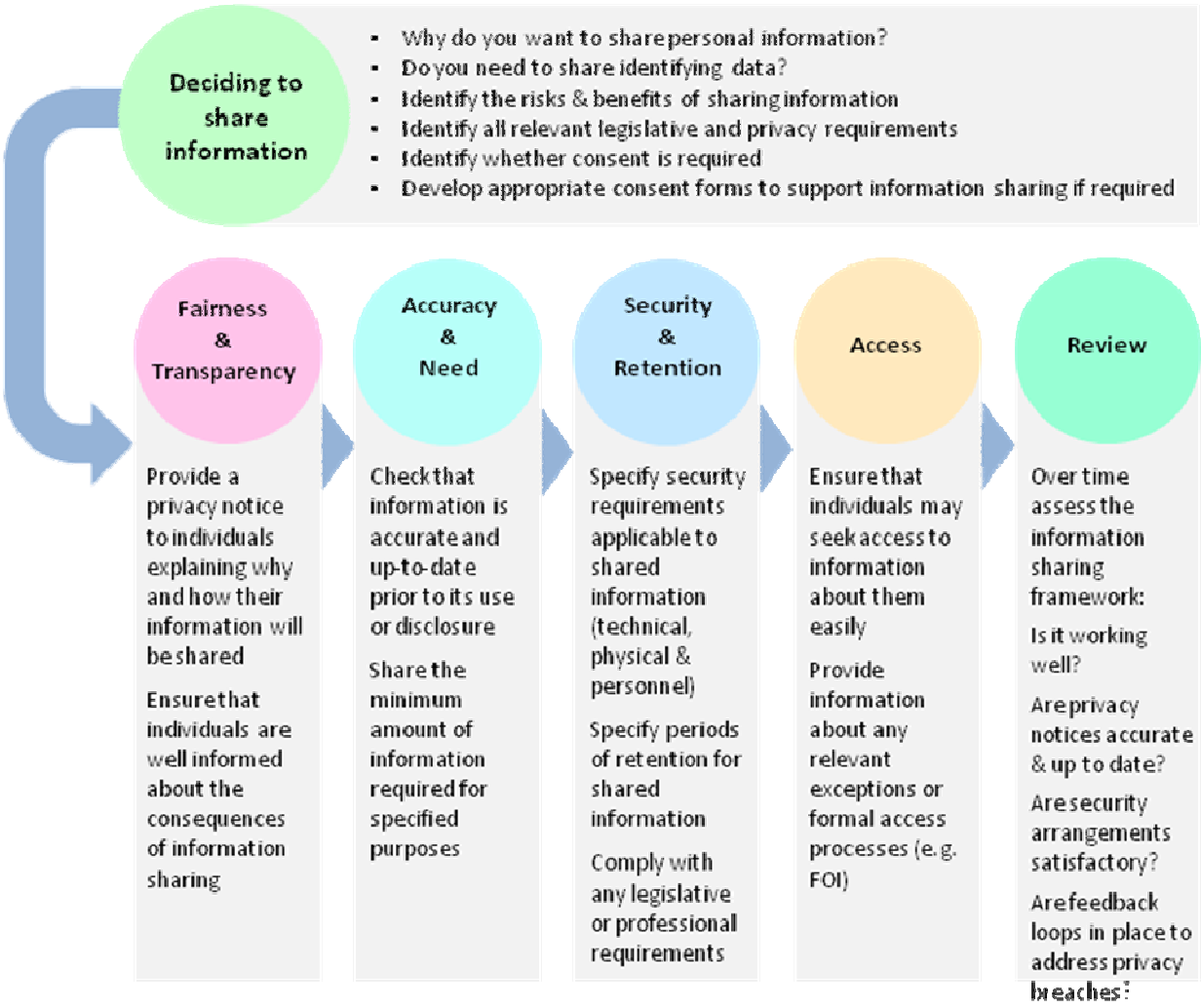
As a starting point, it is important to recognise that a commitment to appropriate information sharing is not mutually exclusive with meeting confidentiality and/or privacy requirements. Rather, the challenge is to undertake a rigorous assessment of information sharing requirements and document a suitable approach to privacy management as part of this process. This may include articulating the objective(s) of any information sharing; identifying

[1] Department of the Attorney General (WA), *Policy Framework and Standards: Information Sharing Between Government Agencies* (2003), p.2, **www.department.dotag.wa.gov.au/_files/Info_sharing_policy.pdf**; Department of Finance and Deregulation, *National Government Information Sharing Strategy* (August 2009), p.24, **www.finance.gov.au/publications/national-government-information-sharing-strategy/docs/ngiss.pdf**.

how it will be achieved; allocating responsibility for the monitoring of privacy practice and compliance; and promoting adherence to the relevant privacy principles.

In Victoria, a number of State and Commonwealth privacy laws apply to the collection and handling of personal information.[2] These laws enshrine privacy principles that are designed to ensure that organisations collect, use, disclose and otherwise handle personal information responsibly and in a way that respects individual privacy. The principles also provide a number of mechanisms that *enable* the sharing of personal information in line with the wishes and expectations of the individual concerned or as otherwise required or authorised by law.

The following diagram provides a high level view of one possible approach to managing the privacy risks posed by information sharing, as well as ensuring that the benefits are identified and realised over time.[3]



[2] *Information Privacy Act 2000* (Vic); *Health Records Act 2001* (Vic); *Privacy Act 1988* (Cth); *Charter of Human Rights and Responsibilities Act 2006* (Vic).

[3] The diagram is based upon information provided in a publication from the UK Information Commissioner's Office: *Framework Code of Practice for Sharing Personal Information* (October 2007), **www.ico.gov.uk**.

Privacy Tenets

Youth Partnerships – Privacy Tenets	
1.	**Commitment to Privacy** Youth Partnerships' stakeholders and participants are committed to protecting the privacy of individuals taking part in the Youth Partnerships initiative. It is recognised that privacy is integral to the success of Youth Partnerships. Wherever possible, Youth Partnerships will seek to promote privacy-positive outcomes. As part of this commitment to privacy, appropriate privacy resources and training through the Office for the Victorian Privacy Commissioner can be organised for Youth Partnerships Project Officers. A strong privacy foundation will support the individual demonstration sites as they implement Youth Partnerships.
2.	**Youth-Centred Focus** Youth Partnerships is a consent-based, youth-centred initiative designed to improve the support offered to individual young people through enhanced information sharing and collaboration. Youth Partnerships will seek to ensure that any activities undertaken for Youth Partnerships are youth centred, based on consent and undertaken transparently and with respect.
3.	**Individual Participation** All Youth Partnership projects will seek to maximise the degree of control young people may exercise over the collection and handling of their personal information as a result of participating in Youth Partnerships. The Youth Partnerships demonstration sites will adopt this principle when developing their work programs and implementation activities.
4.	**Clarity & Transparency of Purpose** Youth Partnerships is committed to clarity and transparency in relation to any collection and handling of personal information under its auspices. An account of the purposes for which personal information may be collected and handled will be documented by the Youth Partnerships project and made available to all relevant stakeholders and participants.
5.	**Accountability** Youth Partnerships will ensure that appropriate governance arrangements are established so as to ensure that these privacy tenets are supported and progressed at the level of each individual Youth Partnerships demonstration site, from development through to implementation.

Frequently Asked Questions - Privacy

What is privacy?

'Privacy' means many different things to people.

It can mean protecting your personal space by not having others observe you when you are at home or in your backyard. It may be expecting not to be subject to video surveillance when you are at work. Central to all ideas of 'privacy' is keeping your own actions, conversations, information and movements free from public knowledge and attention.

What privacy means as a general concept is often different to what privacy means under law. Only certain types of information and activities are protected by privacy legislation.

What sort of information does the Victorian Information Privacy Act protect?

The Information Privacy Act protects “personal information”. This is information or opinion, whether true or not, that is recorded in any form from which a person’s identity is apparent or can be reasonably ascertained.

Note that under this law the information must be recorded. If information is not recorded in some form it is not covered by the Information Privacy Act. However, breaches of the Act can be made when recorded information is disclosed verbally.

Some examples of personal information might be someone’s name, address, sex, age, financial details, marital status, education or employment history. Some personal information is called “sensitive information” and is given special treatment under the Act. This includes information about an individual’s ethnic origin, religious beliefs, sexual preferences and criminal record.

What are information privacy principles?

Information Privacy Principles (IPPs) are the practical core of the Information Privacy Act. With limited exemptions, all Victorian government agencies, statutory bodies and local councils must comply with the IPPs. This is a short summary of the ten Information Privacy Principles:

IPP 1 - Collection

Collect only personal information that is necessary for performance of functions. Advise individuals that they can gain access to personal information.

IPP 2 - Use and disclosure

Use and 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.

IPP 3 - Data quality

Make sure personal information is accurate, complete and up to date.

IPP 4 - Data security

Take reasonable steps to protect personal information from misuse, loss, unauthorised access, modification or disclosure.

IPP 5 - Openness

Document clearly expressed policies on management of personal information and provide the policies to anyone who asks.

IPP 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.

IPP 7 - Unique identifiers

A unique identifier is usually a number assigned to an individual in order to identify the person for the purposes of an organisation's operations. Tax File Numbers and Driver's Licence Numbers are examples. Unique identifiers can facilitate data matching. Data matching can diminish privacy. IPP 7 limits the adoption and sharing of unique identifiers.

IPP 8 - Anonymity

Give individuals the option of not identifying themselves when entering transactions with organisations, if that would be lawful and feasible.

What are data protection laws?

Most privacy laws are more correctly described as data protection laws, as they are limited to regulating the handling of personal information by organisations.

What are other privacy laws protecting Victorians?

Apart from the Information Privacy Act 2000 (Victoria), there are three other main laws which protect the information privacy of Victorians.

The Health Records Act 2001 (Victoria) protects health information handled by the Victorian public and private sectors. “Health information” is defined to include information about the physical, mental or psychological health of an individual, and can include personal information collected in providing an individual with a health service.

The Privacy Act 1988 (Commonwealth) covers the handling of personal information (including health information) by Federal government organisations, credit reporting organisations and parts of the private sector (excluding small businesses).

Under Victoria’s Charter of Human Rights and Responsibilities Act 2006, all Victorian government organisations must act in a way that protects human rights. This includes the right to privacy.

Is privacy the same as confidentiality or secrecy?

Privacy is a separate concept to confidentiality.

What is confidentiality?

Privacy and confidentiality are often thought of as the same and the terms are often used interchangeably. However, confidentiality is a separate legal concept where information is given to a person under an obligation to keep the information confidential (for example, a trade secret, or information confided to someone). Confidential information is usually not available or readily accessible to the public, and may be information which is not recorded in some form.

On the other hand, the IPA protects recorded personal information whenever it is held by the Victorian government or its contracted service providers.

Marking a document with “confidential” or “commercial-in-confidence” will not affect any privacy obligations that might result from use or disclosure of personal information contained within the document.

What is Freedom of Information?

The Freedom of Information Act 1982 (FoI Act), broadly, gives members of the public rights of access and correction in relation to documents about their personal affairs and the activities of the Victorian Government and it’s agencies.

The Act only confers a right of access on the person who is the subject of the personal information, to that person’s own personal information.

The IPA provides that Freedom of Information remains the procedure for people to seek access to their personal information from organisations subject to the FoI Act.

What are some other Australian privacy laws?

Most Australian jurisdictions, except Western Australia and South Australia, have enacted specific information privacy legislation which regulates how certain public and private sector organisations collect, store and handle personal information and provide a mechanism for individuals to make a complaint to an independent Commissioner about a breach of the relevant legislation.

What are some other International privacy laws?

There are various international laws (to which Australia is a signatory) which protect privacy rights. For example, the International Covenant on Civil and Political Rights 1966 contains a general right to privacy which protects areas such as a person's family, home, correspondence and reputation, while the United Nations Convention on the Rights of the Child and Universal Declaration of Human Rights contain similar privacy protections. The Organisation for Economic and Co-operation and Development's guidelines on the protection of privacy and trans-border flows of personal data are cited at the beginning of the Federal Privacy Act 1988.[4]

Frequently Asked Questions – Issues to Consider when Referring Young People to an Outside Agency

When a young person is referred to another outside agency, it is inevitable that personal information about the individual you are referring is disclosed to the agency. The Victorian privacy laws set out the responsibilities and standards for protecting identifiable personal information about an individual from unlawful disclosure, misuse, harm and unauthorised access.

I want to refer a young person to an outside agency - what do I need to consider?

When determining whether to refer a young person to an outside agency, there are four main matters to be addressed.

- Prior consent of the individual for the agency to disclose information about the young person must be obtained;
- Personal information disclosed about that young person to the agency must be up-to-date and current;
- Original files must not be sent to the agency. A photocopy of relevant information about the young person may be disclosed with the prior consent of the young person; and
- A file note of the information disclosed to the agency must be made and documented.

What does consent involve and what are the exceptions when considering consent?

For an individual to consent to the disclosure of his/her personal information, he/she must have legal capacity. To assist in determining if a person is legally capable of making a decision in relation to this issue, the decision maker should consider whether the young person has the mental ability and maturity to understand the nature and effect of his/her decision. For example, a young person who has an impairment which may impact upon his/her legal capacity may not have legal capacity to consent to disclosure of his/her personal information. In making an assessment about capacity, the decision maker must use professional judgment. Professional judgement relates to the position you hold and the duties you are being paid to undertake.

[4] Office of the Victorian Privacy Commissioner, 'Frequently Asked Questions: General Public', http://www.privacy.vic.gov.au/privacy/web2.nsf/pages/frequently-asked-questions-general-public

Consent given by a young person for the disclosure of his/her personal information must be **informed, specific, freely given and current**. *Informed* means the young person has sufficient information to understand the nature and effect of the matter he/she is consenting to. *Freely given* means the young person can make their own decision **free from influences or pressures** which may impair their free will. *Specific* means the consent is not a general all-purpose one, but is **specific to the particular disclosure proposed**. *Current* means the consent must have been given not so long ago that relevant circumstances or the young person's views may reasonably have changed.

Where a young person does not have **legal capacity** because of mental or physical impairment, consent can only be given on their behalf by their legal guardian e.g. a parent or a person appointed as their legal guardian.

Are there any exceptions to disclosure of young person personal information to outside agencies?

If you believe a young person is either at risk or could put others at serious and immediate risk of harm or where a disclosure is necessary to lessen or prevent a serious and imminent threat to an individual's life, health, safety or welfare or where disclosure is required by law or for law enforcement purposes, then the consent of the young person is not required before personal information or the identity of the young person can be disclosed and immediate action should be taken.

We work very closely with some core agencies. Is there anything we can do which supports consistency in information handling of a young person's information?

It is good practice if you are working consistently with an agency that you and the agency enter into a Memorandum of Understanding (MoU) which clearly identifies your information management practices which are consistent with the principles of the Victorian Privacy laws.

Should I keep a record of the young person's information I have shared with outside agencies?

It is important that your practice is transparent and there is a file note or record of the type of information you disclosed to an agency.

Can I send the young person's file to the agency I am referring the young person to?

Once you have consent from a young person, only a copy of the young person's relevant information should be disclosed to the agency to which the young person has been referred. Relevant information is information which is up-to-date and current and relates to the referral i.e. the purpose for contacting the agency. [5]

[5] The information is based upon information provided in a publication from DEECD: '*Student Mapping Tool Privacy Guide* (2010)

Attachment A – Privacy Management Framework Checklist

A Privacy Management Framework (PMF) provides organisations and multi-organisational information-sharing initiatives with a structured approach for the end-to-end and whole-of-life management of the privacy of personal/health information. This is supplemented by the PIA guides and tools provided by the various privacy commissioners.

The PMF allows all stakeholders to identify any gaps in relation to privacy practice. In particular it can highlight the need to develop clear privacy purpose statements and shared documentation and tools (data collection forms, referral forms). Additionally, it assists in determining the legislative requirements for individual projects and emphasizes the need for privacy governance for all involved. The PMF allows for the observation of privacy by embedding the appropriate responsibilities, actions, checks and balances within existing management and risk control functions and activities.

This approach is explained under the following headings:

- Governance and Management
- Information Lifecycle Management
- Risk Assessment and Management
- Systems
- Information Access Control and Security
- Personnel
- Legal
- Privacy Management
- Compliance/conformance/certification
- Tracking, Audit and Reporting
- Persistence Management

Where necessary, initiatives and the organisations should develop a Privacy Management Plan (PMP) which takes the major headings of the PMF and spells out in detail how each requirement will be covered off by the initiative/organisation. The PMP should be a persistent document that forms the basis of the initiative/organisation's ongoing management of personal and health privacy matters.

PRIVACY MANAGEMENT FRAMEWORK CHECKLIST

Program Name	
What is covered by this Checklist – i.e. the whole program or an IT system or an initiative (which could be based around an IT system)?	
Contact Person	
Date of completion	

Privacy Management Framework Principles	Program Response
1. Governance and Management	
a. Is it possible to establish who is responsible for privacy at **program, data collection and systems** level in relation to:	
i. policy	
ii. operations	
iii. audit/control?	

Privacy Management Framework Principles	Program Response
b. Is the policy's coverage explicitly:	
i. **end-to-end** – i.e. across all entities, processes and systems (internal to DHS/DoH or external) that handle personal information that has been captured or created by a DHS/DoH program?	
ii. **whole-of-life** – i.e. from capture/creation through to archiving and eventual destruction?	
c. Do appropriate **feedback loops** exist to:	
i. reaffirm that privacy is being managed effectively	
ii. report breaches?	
2. Information Lifecycle Management	
a. Do **policies, processes and documentary standards** exist that cover information lifecycle management?	
b. Does a **complete and current statement** exist for the program/system/data collection under review of all:	
i. information collected, created, processed, stored and exchanged	
ii. uses/purposes of the information	

Privacy Management Framework Principles	Program Response
iii. entities that handle the information	
iv. the manual and systems processes that handle the information?	
c. Has the **information** been **classified** in accordance with DHS/DoH information classification policy?	
3. Risk Assessment and Management	
a. Does the program actively follow the **DHS/DoH risk assessment and management**:	
i. policies?	
ii. standardised assessment (and response) processes/ methods?	
b. Are **risk assessment (and response) reports** available for the program/s and system/s under review?	
4. Systems	

Privacy Management Framework Principles	Program Response
a. Are **privacy risk assessment and management requirements** embedded into the analysis and **design of systems** (hardware, software, networks, physical environments, etc) at the stages of: i. feasibility ii. design iii. selection (if an external vendor is retained) iv. testing and v. commissioning ?	
b. Are **privacy risk assessment and management requirements** embedded into the **maintenance processes** associated with systems when:	
i. New data fields containing personal information are added	
ii. New functions that impact personal information are introduced	
iii. Data is used for secondary purposes	

Privacy Management Framework Principles	Program Response
c. Are systems subjected to **IT security reviews** as part of:	
i. Development and commissioning?	
ii. Operation?	
iii. Maintenance/modification of key functionality and/or data holdings/management?	
5. Systems Access Control/Security	
a. Have access control requirements for systems been determined by and or assessed based upon an appropriate **IT Security and Identity Management standards and frameworks**?	
b. Are **access control policies and systems** in place to ensure that **only authorised persons** have appropriate access to data collections and the systems that handle these?	
c. Are **audit trails/reports/documents** available to **evidence**:	
i. **Appropriately authorised** registration, enrolment, maintenance and deregistration processes have been followed for all system users?	

Privacy Management Framework Principles	Program Response
ii. **Delegated managers** (within or outside of the program) **have regularly sighted** and signed off on the user access permissions under their control?	
6. Personnel	
a. Within the Program	
i. Do **personnel (staff/contractor) contracts** include stipulations regarding protection of privacy of personal information that will be dealt with in the course of the person's job?	
ii. Is **awareness raising and education** provided on this topic including refresher training?	
iii. Are **effective sanctions** available and enforced?	
b. External to the Program	
i. Are external organisations required to attest to the fact that **staff/contractor contracts** include provisions/obligations regarding protection of privacy of personal information that will be dealt with in the course of the person's job?	
ii. Is **awareness raising and education** provided on this topic including refresher training?	

Privacy Management Framework Principles	Program Response
iii. Are **effective sanctions** available and enforced?	
7. Legal	
a. Do **contracts with external parties** stipulate responsibility for end-to-end and whole-of-life management and protection of personal/sensitive information that is collected, created, accessed, received, etc?	.
b. Do processes exist to determine **legal restrictions and/or compliance requirements** in relation to e.g. **main legislation/regulation** covering DHS/DoH functions, Health Records Act, Information Privacy Act, Commissioner for Law Enforcement Data Security Act, Privacy Act 1988, etc	.
8. Privacy Management	
a. Framework	
i. Does the program have a **formal Privacy Management policy** and set of methods?	
ii. Have these been applied to the program/system under review?	

Privacy Management Framework Principles	Program Response
iii. Do **Privacy Statements** exist in relation to the core elements of the program/system under review?	
iv. Have **Privacy Reviews and/or Privacy Impact Assessments** been undertaken at the appropriate check-points e.g.: ➔ If no privacy review has ever been undertaken previously. ➔ If new data collections or systems or programs or initiatives that involve collection and/or handling of personal data are introduced ➔ If significant data collection and/or systems changes/additions are undertaken ➔ If machinery of government changes result in the movement of personal data to another department.	
b. Identifiers	
i. Are **unique and persistent identifiers** allocated to personal data?	
ii. Are there **explicit consent and usage protocols** associated with the use of such identifiers?	
iii. Is the **use of such identifiers outside of the immediate context** controlled and monitored?	

Privacy Management Framework Principles	Program Response
c. Consent	
i. Does the program have **defined consent protocols** for data collections that contain personal information?	
ii. Do information collection processes (whether based upon individuals completing forms, or by way of phone or counter interviews) include **disclosure** to the individual **of the primary** (and, if applicable, **secondary**) **purposes** of the collection, and is consent obtained from the individual or their representative?	
9. Compliance/certification	
a. Do formal **privacy compliance/certification methods** exist in relation to processes and systems across the information management lifecycle?	
b. Are the **results** of the application of these methods available for the program/system under review?	
10. Tracking, Audit and Reporting	
a. Is all **access to data stores logged** in sufficient detail to enable a determination to be made regarding which user conducted what access when?	

Privacy Management Framework Principles	Program Response
b. Do processes exist to **identify and report breaches** to nominated roles within the program, within DHS/DoH and if necessary to the Health Records Commissioner, Office of the Victorian Privacy Commissioner and Police?	
c. Are **periodic independent reviews** undertaken to determine the efficacy/compliance of privacy management – e.g. as part of internal and/or external audit processes?	
11. Persistence Management	
a. Do processes/mechanisms/strategies exist to ensure **persistence of all policies, processes, standards, documents** etc in the event of:	
i. loss of key personnel	
ii. machinery of government changes	
iii. loss/destruction of key paper/systems resources	
iv. changes in technology (e.g. data storage technology)?	

Attachment B – Youth Partnerships Privacy Impact Assessment Report

BAINBRIDGE
associates

VICTORIAN GOVERNMENT

DEPARTMENT OF EDUCATION & EARLY CHILDHOOD DEVELOPMENT

Youth Partnerships Secretariat

Youth Partnerships Privacy Impact Assessment (PIA) Report (v.1.0)

The contact person for this report is:

Dr Bridget Bainbridge

Director

Bainbridge Associates Pty Limited

M: 0435 358 803

bridget@bainbridgeassociates.com.au

Table of Contents

Executive Summary

The *Youth Partnerships* Secretariat of the Department of Education and Early Childhood Development (DEECD) engaged Bainbridge Associates Pty Limited to undertake a Privacy Impact Assessment (PIA) of the *Youth Partnerships* initiative in September 2011.

The PIA was undertaken from September – December 2011. A Youth Partnerships PIA Workshop involving key stakeholders was held on 8 December 2011, allowing stakeholders to provide feedback on the PIA's preliminary findings and proposed recommendations.

The Youth Partnerships PIA Report was finalised in January 2012, taking account of the feedback provided at the PIA workshop.

Overview

The *Youth Partnerships* initiative was established to 'design and test new ways for the education, youth and family support, justice, homelessness and mental health sectors to work more collaboratively to support individual young people experiencing problems'.[6] It is a complex, whole-of-Victorian-Government (WOVG) initiative involving seven demonstration sites – each with multiple participants – and traversing a number of regulatory frameworks, including privacy.

The PIA finds that *Youth Partnerships* is capable of complying fully with privacy requirements. It also confirms that *Youth Partnerships* has a high privacy risk profile – both in terms of privacy law compliance requirements and what may be termed 'privacy perceptions'. It is critical that both of these aspects of privacy are managed effectively throughout the life of *Youth Partnerships* in order to ensure that privacy does not become an impediment to its successful implementation.

The PIA finds that *Youth Partnerships* is not sufficiently advanced to undertake a comprehensive PIA at this point in time. However, it is equally clear that a number of practical steps can be taken immediately to build a strong privacy foundation for *Youth Partnerships*. It is considered that the development of a strong, consistent privacy foundation across the entirety of the *Youth Partnerships* initiative should form the key priority for the *Youth Partnerships* Secretariat and the demonstration sites at this point in time.

Summary of Key Findings

At a high level, no critical or 'drop dead' privacy issues were identified during the PIA process. In particular, the proposed consent-based and young-person centred approach is consistent with good privacy practice and compatible with the requirements of privacy principles contained in privacy legislation.

It is clear that 'privacy' is an over-determined term in the *Youth Partnerships* context, functioning as a shorthand reference to a wide range of issues only some of which are specifically related to information privacy and the requirements of privacy legislation. It is considered that this arises as much from a lack of knowledge about privacy as it does from any complexity involved in *Youth Partnerships*.

The PIA finds that privacy is not antithetical to *Youth Partnerships*; good privacy practice will help, not hinder, the delivery of better, more coordinated, youth services. However, a concerted effort is required to ensure that privacy functions as a positive rather than a

[6] DEECD website, Youth Transitions, *Youth Partnerships: coordinating services to help young people stay on track,* http://www.education.vic.gov.au/sensecyouth/youthpartnerships/default.htm

negative for *Youth Partnerships*. In particular, investing in the development of a sound understanding of privacy across the *Youth Partnerships* network will help participants (at a governance, organisational and individual level) feel confident that privacy has been accounted for and, perhaps more importantly, that privacy has been built into the initiative as a whole, not bolted on afterwards.

In order to achieve this, it is recommended that *Youth Partnerships*:

- Commits to seeking effective privacy outcomes as a core component of the delivery of *Youth Partnerships*;
- Develops a working understanding of the meaning of privacy (both in terms of privacy legislation and privacy practice) and communicates that effectively to *Youth Partnerships* participants, including through privacy training;
- Develops holistic *Youth Partnerships* policies and procedures designed to manage privacy effectively; and
- Adopts a critical approach to the characterisation of issues as being '*because of privacy*', particularly where this prevents information sharing or other necessary actions.

In practical terms, building upon the findings of PIA process, this may comprise:

- The development of a shared set of privacy tenets to guide the demonstration sites as they engage with *Youth Partnerships;*
- The implementation of a *Youth Partnerships* Privacy Management Framework to help the demonstration sites take a common approach to privacy management, including consistent documentation of key requirements (legislative, technical, policy, etc.) even as their various implementation activities diverge;
- The incorporation of relevant privacy content into the *Youth Partnerships* Common Practice Framework; and
- The provision of privacy training across the demonstration sites to raise awareness of privacy in a positive way.

This set of proposals was discussed with key stakeholders at the December 2011 workshop. Overall, there was strong support for pursuing each of them as part of a holistic *Youth Partnerships* privacy strategy. However, it is strongly recommended that – as much as possible – *Youth Partnerships* seeks to take ownership of these concepts or approaches rather than simply adopting them. True success lies in making privacy an inherent part of everyday business. To do this successfully will require input and debate from *Youth Partnerships* participants, not just the commissioning of external privacy advice and consultation around privacy.

It is also necessary to acknowledge that the *Youth Partnerships* initiative is complex, for a range of reasons. These include:

- Australia's 'patchwork' of privacy regulation results in the application of multiple privacy regimes to the *Youth Partnerships* initiative despite it being a WOVG initiative and, ostensibly, subject to Victorian privacy laws.
- *Youth Partnerships* operates in a complex regulatory environment comprising a broad mix of 'governing' and privacy legislation. In terms of the interaction between privacy and other laws, governing legislation will override privacy legislation to the degree of any inconsistency. This privacy 'override' – in which other legislative provisions may outweigh or override privacy at the level of obligation, authorisation and permission – introduces additional complexity.

- The funding arrangements for the provision of youth services across Victoria are mixed and include both Victorian and Australian government funding. This complicates privacy compliance in terms of *Youth Partnerships* because of the impact of outsourcing provisions designed to ensure that privacy protection 'follows the data'. The outsourcing provisions contained in privacy legislation, while understandable in policy terms, result in a more complex privacy compliance environment.
- Privacy compliance is focused upon individual organisations – i.e. privacy obligations apply at the level of the organisation, not at the level of an initiative. This means that multi-party WOVG initiatives are not readily 'accommodated', requiring additional care in order to ensure that an appropriate 'umbrella' of privacy management is in place. In terms of responsibility for *Youth Partnerships* privacy compliance, this lies with DEECD, as it has been designated lead agency and this is where the *Youth Partnerships* Secretariat is based. However, at the level of governance, responsibility lies with the Children's Services Coordination Board.

In an ideal world it would be preferable to remove this level of complexity from *Youth Partnerships*, but it is simply not possible to do so within the current legislative environment. Therefore, a key requirement for *Youth Partnerships,* particularly at the governance and secretariat levels is to seek to provide *Youth Partnerships* participants with the tools to understand and manage this complexity as efficiently as possible.

It is considered that a commitment to good privacy practice – accompanied by a range of supportive privacy tools, policies, procedures and training – will ensure that *Youth Partnerships* is in a strong position to achieve a high level of privacy compliance. However, it must be noted that:

- Privacy is a human right and *Youth Partnerships* must be consistent with the Victorian *Charter of Human Rights and Responsibilities* as well as information privacy requirements.
- *Youth Partnerships* will involve the collection and handling of a wide range of personal information, including sensitive and health information and information about family members. This information will be shared (with consent) more broadly across multiple organisations, increasing both the amount of information collected and handled and the capacity for a privacy breach. A failure to protect this information may result in breaches of individual privacy. While there are some remedies available under privacy legislation, essentially, once privacy is breached, it cannot be restored and the consequences of a breach may be significant.
- There is always a capacity for privacy breach as a result of human error. The challenge for *Youth Partnerships* is to institute an environment in which this is mitigated against as much as possible so that the potential for a privacy breach is minimised and, in the event of a breach, effective feedback loops ensure appropriate action is taken as quickly as possible.

Summary of Recommendations

The *Youth Partnerships* PIA produced 5 recommendations, listed below. Comments about each recommendation are found in the relevant section of the full report (referenced below).

Recommendation 1
It is recommended that a summary of relevant privacy findings from previous youth services initiatives, including the Better Youth Services Pilots are documented and used explicitly to

inform the current *Youth Partnerships* process.

Section 3.4.1 p.16.

Recommendation 2

It is considered that the primary privacy focus for *Youth Partnerships* at this point in time is to develop a strong privacy foundation capable of sustaining and guiding the activities of the seven demonstration sites operating under the *Youth Partnerships* umbrella.

It is recommended that *Youth Partnerships* takes the following practical steps towards achieving this aim:

1. Development of a shared set of *Youth Partnerships* privacy tenets to guide the demonstration sites as they engage with *Youth Partnerships;*
2. Implementation of a *Youth Partnerships* Privacy Management Framework to help the demonstration sites take a common approach to privacy management, including consistent documentation of key requirements (legislative, technical, policy, etc.) even as their various implementation activities diverge;
3. Incorporation of relevant privacy content into the *Youth Partnerships* Common Practice Framework; and
4. Provision of coordinated privacy training across the seven demonstration sites.

Section 2.5, p.18.

Recommendation 3

It is recommended that explanatory, high-level information about the Australian 'privacy patchwork' and its impact is provided in the Common Practice Framework.

More detailed information about the approach to managing this patchwork may be provided via the *Youth Partnerships* website.

Section 3.4.1, p.23.

Recommendation 4

It is recommended that steps be taken to identify and document the main instances of 'privacy override' that will occur in the *Youth Partnerships* context to inform participants about their impact.

While the Common Practice Framework is not a suitable home for such detailed privacy information, it is considered that relevant information may be provided via the *Youth Partnerships* website (under a privacy management heading).

Section 3.4.2, p.24

Recommendation 5

It is recommended that the privacy information developed for the *Youth Partnerships* Common Practice Framework take a 'highest common denominator' approach to privacy principles, providing a generic account of the privacy principles that is designed to increase knowledge about the information lifecycle enshrined within the privacy principles rather than describing the specific detail of, for example, the Victorian IPPs or HPPs.

In due course, participants should be provided with more detailed information about the specific privacy principles applicable to *Youth Partnerships* as a WOVG initiative via the *Youth Partnerships* website.

Section 3.4.3, p.26.

Introduction

Youth Partnerships – Project Requirements

The *Youth Partnerships* Secretariat of the Department of Education and Early Childhood Development (DEECD) engaged Bainbridge Associates Pty Limited to undertake a Privacy Impact Assessment (PIA) of the *Youth Partnerships* initiative in September 2011.

It was specified that the PIA must:

- Identify the scope and impact of privacy legislation – in particular, the *Information Privacy Act 2000* (Vic) (IPA) and the *Health Records Act 2001* (Vic) (HRA) – upon the *Youth Partnerships* initiative; and
- Recommend ways to mitigate or otherwise manage identified privacy risks.

It was also envisaged that the results of the PIA would contribute to the development of privacy content and guidance for a Common Practice Framework being developed as part of the *Youth Partnerships* initiative.

What is a PIA?

A PIA is a point-in-time assessment of the actual and/or potential privacy impacts that an existing or proposed initiative, system, data collection or program may entail. It is a systematic process that takes account of the collection and handling of personal information (including sensitive and health information).

A PIA highlights any unacceptable privacy risks. It includes recommendations to mitigate negative impacts where possible, as well as identifying ways to promote privacy positive outcomes. In essence, a PIA provides assurance to an organisation that a project:

- *Complies with privacy law requirements; and*
- *Does not raise significant privacy policy concerns that cannot be mitigated.*

A PIA is a privacy risk management tool that is particularly useful at the beginning of a project's development phase. By helping to identify privacy risks and potential mitigation strategies, it ensures that privacy is taken into account from the very beginning, increasing the likelihood that the final project will be 'privacy savvy'.

In addition to identifying privacy issues, a PIA also focuses attention upon privacy-positive solutions; it seeks valuable input and buy-in from stakeholders via consultation and helps to embed a privacy management focus that can be maintained throughout the life of the project (from development through to implementation and then 'business as usual'). A PIA provides a structured and repeatable assessment tool that, in the case of complex initiatives, may be undertaken on a number of occasions.

At a minimum, a successful *Youth Partnerships* PIA would be expected to:

- Identify all relevant privacy obligations, risks and issues;
- Map information flows of personal information against the requirements of the relevant sets of privacy principles;
- Enable constructive privacy consultation with key stakeholders;
- Recommend a privacy management approach to avoid/mitigate privacy risks;

- Identify privacy positive outcomes wherever possible; and
- Contribute to an ongoing privacy assurance program, including via the proposed Common Practice Framework.

PIA Methodology

In April 2009, the Office of the Victorian Privacy Commissioner (OVPC) published *Privacy Impact Assessments: A Guide for the Victorian Public Sector* (edition 2).[7] This guide was developed in the context of the IPA, but it is also broadly applicable to the HRA. In May 2010, the (then) Office of the federal Privacy Commissioner published a revised version of its *Privacy Impact Assessment Guide*, which is applicable to public and private sector organisations.[8]

Bainbridge Associates broadly adopts the OVPC PIA methodology whenever a PIA is conducted for a Victorian public sector organisation or involves a WOVG initiative. Material from the federal PIA guide and other bespoke privacy tools may also be used as relevant.

Recognising that there is no 'one size fits all' PIA, the degree to which the OVPC's methodology is adopted and/or adapted depends upon the specific circumstances of each particular project. However, as a starting point, Bainbridge Associates works with the following PIA structure:

- Describe the project;[9]
- Describe the information flows (of personal information);
- Analyse the information flows against the requirements of the *Information Privacy Act's* Information Privacy Principles (IPPs) and the *Health Records Act's* Health Privacy Principles (HPPs), as relevant;
- Analyse the privacy control environment; and
- Document the findings and recommendations in a PIA report.

The *Youth Partnerships* PIA was conducted from September – December 2011. A workshop was held with key stakeholders on 8 December 2011 to review the PIA's preliminary findings and recommendations. The *Youth Partnerships* PIA Report was finalised in January 2012, taking workshop feedback into account.

The *Youth Partnerships* PIA Report does not constitute legal advice.

[7] OVPC, *Privacy Impact Assessments: A Guide for the Victorian Public Sector*, edition 2 (April 2009), www.privacy.vic.gov.au/privacy/web2.nsf/files/privacy-impact-assessments-guide.
[8] OPC, *Privacy Impact Assessment Guide* (May 2010), http://www.privacy.gov.au/materials/types/guidelines/view/6590.
[9] The PIA report must operate as a stand-alone report that may be read by any interested party without detailed knowledge of the initiative.

Youth Partnerships and Privacy

What is *Youth Partnerships*?

Youth Partnerships is a Victorian Government initiative established to 'design and test new ways for the education, youth and family support, justice, homelessness and mental health sectors to work more collaboratively to support individual young people experiencing problems'.[10] Over a three-year period, it is envisaged that *Youth Partnerships* will support service providers operating in these sectors to work together to ensure:

- A greater focus on early intervention;
- Consistent approaches to assessment and referral of young people across these sectors; and
- Clear entry points into the right youth services at the right time, including tailored education options.

The initiative is being implemented via seven demonstration sites across metropolitan and rural/regional Victoria. The sites are based on groupings of Local Government Areas (LGAs), thus the boundaries involved are multi-LGA rather than single LGA. The demonstration sites are:

1. Greater Geelong, Queenscliff and Surf Coast
2. Yarra Ranges, Maroondah and Knox
3. Frankston and Mornington Peninsula
4. Swan Hill, Gannawarra, Buloke and Mildura
5. Ballarat, Hepburn, Pyrenees, Moorabool, Golden Plains
6. Greater Bendigo, Central Goldfields, Mount Alexander, Campaspe, Macedon Ranges and Loddon
7. Wyndham and Hobsons Bay

While *Youth Partnerships* is a relatively new initiative, it builds upon a significant body of prior work, including the Better Youth Services Pilots and the Vulnerable Youth Framework.

Youth Partnerships and Privacy

Youth Partnerships operates in a complex, multi-party environment and involves numerous organisations including Victorian government departments and agencies, local government and contracted service providers (non-government or not-for-profit sector). The funding arrangements for youth services are complex, involving multiple funding sources and service agreements.[11] The regulatory backdrop to this environment is likewise complex, involving a range of 'governing' legislation in addition to Victorian and Commonwealth privacy legislation.

Against this backdrop, *Youth Partnerships* is about enabling the best possible 'holistic' care to a young person who may be/is 'at risk', based upon a client-centred model of care. This is

[10] DEECD website, Youth Transitions, *Youth Partnerships: coordinating services to help young people stay on track,* http://www.education.vic.gov.au/sensecyouth/youthpartnerships/default.htm

[11] See, for example, Productivity Commission, *Contribution of the Not-For-Profit Sector* (February 2010), in particular, Chapter 11 – Direct Government Funding and Chapter 12 – Delivery of Government Funded Services: http://www.pc.gov.au/projects/study/not-for-profit/report. See, also, Department of Planning and Community Development, *Common Funding Agreement*: http://www.dpcd.vic.gov.au/communitydevelopment/community-sector/ocs-initiatives/common-funding-agreement.

defined against current arrangements in which a young person may have to 'navigate' a range of service providers in order to seek coordinated advice and/or services. In some instances, as a result of a lack of information sharing, young people seeking assistance are required to visit multiple organisations, repeating their story multiple times. The difficulty in obtaining help may lead to further disengagement and so on.

In order for *Youth Partnerships* to be successful, personal information about individual young people will need to be shared across services. This information may include:

- Identity and location
- Health and/or wellbeing status
- Legal status
- Family background
- History of involvement with other services

As a result, *Youth Partnerships* is reliant upon the collection, use, disclosure and handling of young people's personal information, including health and sensitive information and information about third parties (family members). Therefore, it raises a number of legitimate questions and compliance requirements relating to privacy that need to be canvassed and managed appropriately over the life of the project. It also squarely raises issues around the degree to which *governing* legislation, rather than privacy laws, may impede information sharing or otherwise impact on privacy requirements.

In terms of the PIA, *Youth Partnerships'* privacy risk profile is categorised as 'high', for the following reasons:

- Personal information is the *lifeblood* of the *Youth Partnerships* initiative;
- *Youth Partnerships* involves the *collection* of a wide range of personal information about *young people* and their *families* by multiple organisations;
- *Youth Partnerships* may involve the collection of *health information* and *sensitive information*, both of which are subject to additional protection under privacy legislation;
- *Youth Partnerships* will involve the *disclosure* of personal information beyond organisational boundaries, which raises issues around consent; and
- *Youth Partnerships* functions in a *complex regulatory environment*, of which privacy is merely one component, albeit an important one.

Privacy laws, and the privacy principles they embody, contain a number of mechanisms that *enable* personal information to be collected, used, disclosed and otherwise handled in order to facilitate specific information flows, primarily through consent but also through notification and transparency mechanisms or as authorised by law.

While *Youth Partnerships* may be assessed as having a high privacy risk profile, it is not the case that privacy law necessarily presents an impediment to information sharing between and across multiple youth service providers, in line with a young person's expressed wishes. Rather, the key is to ensure that any information sharing occurs appropriately, in accordance with privacy requirements and privacy mitigation strategies, established guidelines and governance arrangements.

Is 'privacy' a problem?

One of the reasons for commissioning a *Youth Partnerships* PIA was that prior feedback from stakeholders, over a number of years, regularly identified 'privacy' as a potential impediment to information sharing in a youth services context. A PIA was viewed as having the capacity to

provide greater clarity, particularly in relation to identifying areas where information should not be shared. It was considered that this would enable the *Youth Partnerships* demonstration sites to develop their project plans with greater confidence.

While the *Youth Partnerships* PIA finds that privacy has functioned as a recurrent issue in the youth services' context, it was not clear at the beginning of the PIA process whether the privacy issues were 'real' (i.e. specific privacy law compliance impediments exist), 'perceptions' (i.e. no privacy law compliance issues can be identified but the project nevertheless makes participants feel uncomfortable about the way in which personal information is to be collected and handled) or a mixture of the two.

A key focus in the early stages of the *Youth Partnerships* PIA involved ascertaining the scope and specific nature of the privacy issues posed by *Youth Partnerships.* Each demonstration site was asked to complete a preliminary privacy survey, which was designed to:

- Provide a snapshot of current local governance arrangements;
- Document current project plans and specific *Youth Partnerships* implementation sites' initiatives;
- Identify any privacy protocols/policies developed to support *Youth Partnerships;* and
- List specific privacy impediments or privacy issues relating to *Youth Partnerships.*

While all of the sites were able to account for governance arrangements (a positive finding), the survey responses also illustrated that there is a wide variation between the sites in terms of the maturity of their project planning and implementation processes.

Some of the sites are at a very early stage of development. As a result, they are not in a position to provide a detailed account of privacy as it relates to their activities, either in terms of specific privacy issues or in relation to privacy management. Others, while more developed, are still not at the point of documenting a mature approach to privacy management, e.g., no *Youth Partnerships* privacy policies have been drafted.

Further, the survey results demonstrated that *Youth Partnerships* is not a distinct, stand-alone initiative in its own right. Rather, it is a framework within which multiple demonstration sites have been funded to explore better, more coordinated and youth-centred ways to deliver youth services. In that sense, the initiative '*Youth Partnerships'* cannot function as an object of assessment. It is better characterised as a conceptual framework or governing principle.

Notably, the survey did not produce a significant list of 'privacy problems' from the demonstration sites. On the whole, any privacy problems identified were generic rather than specific (e.g. multiple organisations participate in *Youth Partnerships*; they have varying levels of privacy knowledge and tend to adopt a risk-averse approach to information sharing as a means of mitigating potential – i.e. unknown – privacy risks).

While there is recognition that privacy legislation is relevant to *Youth Partnerships,* the practical impact of privacy requirements is not familiar or widely understood. So too, the interaction between privacy legislation and other more specific 'governing' legislation is viewed as complex and lacking clarity. For example, the interaction between privacy requirements and the *Children, Youth and Families Act 2005* (Vic), particularly in relation to disclosure without consent, was noted as an area requiring clarification even though this is not a specific issue raised by *Youth Partnerships*.

A lack of understanding of basic privacy requirements or confusion about legislative precedence vis-à-vis privacy and other laws not surprisingly may result in risk-averse behaviour. Such behaviour may be ascribed to 'privacy' regardless of whether or not privacy is

the cause of the problem. This bundling of a range of regulatory and other issues under the rubric 'privacy' results in 'privacy' being an over-determined term requiring a healthy degree of scepticism.

While the survey was preliminary in nature, it suggested that the *Youth Partnerships'* 'privacy problem' is a combination of 'real' and 'perceived' privacy issues. Subsequent consultation activities undertaken during the PIA process confirmed that the 'privacy problem' is a combination of real and perceived privacy issues and, therefore, any attempts to deal with privacy must take account of both of these elements.

It is clear that *Youth Partnerships* operates in a complex regulatory environment. As a result, over the life of *Youth Partnerships* it is expected that specific *privacy* compliance issues will be identified and that some of these issues may pose genuine impediments. At other times compliance issues arising from legislative interactions will need to be assessed carefully in order to develop an appropriate response that, wherever possible, supports the objectives of *Youth Partnerships*. Sometimes, these may prevent information sharing on non-privacy grounds.

Likewise, it is clear that privacy perceptions (or, equally, privacy *mis*conceptions) are present in *Youth Partnerships*. While the privacy perceptions identified during the PIA process were expressed at a generic level, the effects of these may prove problematic if not tackled effectively at an early stage of a project's development. There is a risk that privacy misconceptions may become embedded over time, in practice resulting in risk-averse approaches to information sharing. In privacy circles, this behaviour is encapsulated by the acronym BOTPA: 'because of the Privacy Act'.

BOTPA describes a scenario in which privacy is used as an excuse 'to justify inaction or non-cooperation'.[12] While this is sometimes caused by ignorance, it may also be used deliberately to prevent a particular outcome. Whatever the reason, an information-intensive initiative like *Youth Partnerships* needs to take steps to mitigate against BOTPA, in particular by building a strong privacy foundation designed to minimise privacy risks at both the level of compliance *and* perception.

Inability to conduct a full PIA for *Youth Partnerships*

PIAs have become increasingly popular as a key privacy risk management tool, both within Australia and internationally. While there is no legislative requirement under Victorian or Commonwealth privacy laws to conduct a PIA, in some circumstances PIAs have become a de facto privacy compliance mechanism.

There is no 'one size fits all' PIA. When an organisation commissions a PIA, it needs to consider what type of PIA is most appropriate to the project and likely to deliver the best value. In the case of *Youth Partnerships*, an external, full PIA was commissioned with the expectation that it was feasible to conduct a full PIA. In part, this followed on from the Better Youth Services Pilots, where the desirability of conducting a state-wide PIA was identified as a key finding but, at the same time, it was not clear to stakeholders what a PIA involved or how to go about undertaking one.

However, in order to undertake a full PIA, a number of threshold and other requirements need

[12] See, for example, Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report 108 (May 2008), Volume 1, p.109. See, also, Australian Privacy Foundation, 'BOTPA – Blame it on the Privacy Act', http://www.privacy.org.au/Resources/BOTPA.html.

to be taken into account.[13]

Threshold requirements

An effective PIA assesses the technical, policy, legal and governance components that comprise an initiative *as a whole*. In essence, this means assessing an initiative 'end-to-end' and from a 'whole-of-information-lifecycle' perspective:

- The term *'end-to-end'* is intended to convey the idea that *Youth Partnerships* needs to understand and account for the continuum of entities, processes and systems across the youth services community that will collect and handle personal information as a direct or indirect consequence of *Youth Partnerships*.
- The term *'whole-of-information-lifecycle'* is intended to convey the idea that *Youth Partnerships* needs to understand and account for the entire lifecycle of personal information from collection through to archiving and destruction.

If there is insufficient information available about an initiative, it is not possible to provide a full account of the potential privacy impacts. So too, if the PIA scope is circumscribed or restricted, it will only address a 'segment' of the information lifecycle associated with an initiative, which risks producing a misleading or inaccurate privacy assessment.

Finding

There is insufficient information available about *Youth Partnerships* as a whole to support an end-to-end and whole-of-information-lifecycle assessment at this point in time. Nor are any of the demonstration sites sufficiently advanced to enable a site-specific PIA.

An effective PIA must be *fit for purpose*. There is no 'one size fits all' PIA; depending on the circumstances, it is possible to conduct an internal, high-level, preliminary PIA all the way through to an externally-conducted, full PIA involving public consultation. This means that each organisation must determine the best approach and tailor the PIA process accordingly. For example, if a project is in the early stages, it may not be useful to undertake a full-scale PIA involving public consultation process. If a project has not been fully endorsed or there is a lack of clarity about its status, it may be unwise to proceed with a full PIA. If a project is close to implementation, a preliminary PIA will not be appropriate. If a project involves redevelopment or an extension of current functionality, it may be appropriate to focus upon the delta between the current status and the 'to be' status.

Finding

Youth Partnerships is at an early stage of development. Many of the demonstration sites are still in the process of developing project plans. In these circumstances, it is most appropriate to conduct a threshold PIA, which aims to help ensure that the best privacy foundation is in place so that privacy issues may be identified as early as possible and actioned consistently/as needed.

Youth Partnerships follows on from a number of previous government initiatives seeking to improve the delivery of youth services in Victoria. In order to prevent 're-identifying' the

[13] The following section is partly based on findings from a recent preliminary privacy survey undertaken for DEECD in relation to the Enterprise Reporting and Business Intelligence (ERBI) platform. As these findings are equally relevant to *Youth Partnerships,* additional analysis has been included in this report.

privacy wheel, a stocktake of previous youth-oriented pilots and consultation processes should be undertaken, documented and used to inform *Youth Partnerships*. In particular, it is noted that the Better Youth Services Pilots generated a large number of findings, including identifying areas where further work was required such as privacy.

Recommendation 1

It is recommended that a summary of relevant privacy findings from previous youth services initiatives, including the Better Youth Services Pilots are documented and used explicitly to inform the current *Youth Partnerships* process.

Other PIA Considerations

A PIA necessarily focuses upon privacy issues. Therefore, it provides a *specific view of an initiative* (albeit a particularly important one), mapping an initiative's information flows against a set of information privacy principles. Clearly, a government initiative must comply with all relevant legal requirements, including privacy requirements. However, privacy is not absolute – in certain circumstances it is legitimate for an organisation to weigh privacy risks against other competing public interests or desired outcomes. Organisations have a responsibility to take account of the entire set of applicable governance, policy, legal and technical issues – not just privacy – some of which may conflict with the recommendations arising from a PIA.

Finding

As *Youth Partnerships* is at an early stage of development this will not be a pressing issue in the short term. However, it is important to ensure that this is kept in mind as *Youth Partnerships* commences implementation activities via the demonstration sites.

Wherever possible, *Youth Partnerships* should seek to identify outcomes that support both privacy and information sharing but, in recognition of the fact that privacy is not an absolute right, the public interest in improving the delivery of youth services, especially to vulnerable youth, may outweigh the public interest in protecting privacy in certain circumstances.

It is considered that having a strong privacy foundation in place will help to ensure that any 'balancing' assessment is appropriately informed by privacy considerations without being overwhelmed by them.

A PIA is best conducted prior to implementation. This is designed to ensure that positive and negative privacy outcomes are identified and actioned – promoted, mitigated or resolved at an early stage. This is particularly critical when IT systems are involved as retrofitting may prove to be prohibitively expensive. Any residual privacy risk is problematic, however, as it will contribute to a diminution of trust in the initiative. When undertaking a PIA post-implementation, there is always a risk that it may identify issues that should have been resolved prior to implementation, resulting in the need for remediation.

Finding

Youth Partnerships has commenced its privacy work sufficiently early that privacy may be factored into project planning and a coordinated approach developed to accommodate the multiple demonstration sites.

At this point, no proposals involving ICT as a means of promoting information sharing are under development, although it is envisaged that they may be in the future (subject to funding). It is considered that the development of an appropriate privacy foundation will assist in the management of any future privacy issues that arise as the result of developing an ICT solution for *Youth Partnerships*.

A PIA is a *point-in-time* assessment. It is not capable of managing privacy over time. A comprehensive privacy management framework is needed to ensure that privacy is managed effectively and actively both pre- and post-PIA. A PIA is best viewed as a component of an overarching approach to privacy, not a stand-alone solution to a particular privacy problem or an end in itself. Further, in certain circumstances – e.g. the development of complex information-sharing initiatives – a number of PIAs may be undertaken throughout the development cycle.

The management of *Youth Partnerships'* privacy issues is expected to be challenging because of the fact that the multiple demonstration sites will develop their projects independently, focusing upon the issues that are most relevant at the local level. The strength of this approach is that it will enable multiple options to be explored in the short-medium term, providing a richer evidence base for the prospective rollout of additional *Youth Partnership* sites across Victoria in the future.

Finding

While it is not necessary for all of the sites to be undertaking the same implementation activities, it is important that there is a means of gathering information about privacy issues from each of the sites in a systematic and consistent way.

Conclusion and Recommendations

Conducting a PIA involves developing a privacy narrative about a particular initiative. By 'telling the privacy story', a PIA helps a broader range of stakeholders understand what is at stake from a privacy perspective (particularly when technical issues are involved), as well as the options that may be available to mitigate privacy risk and – at times – enhance privacy. Additionally, a PIA may provide an opportunity to increase knowledge about privacy and privacy management strategies amongst stakeholders and participants.

Fundamentally though, if the information flows of personal information involved in each of the demonstration sites cannot be documented, it is not possible to map these against the requirements of the applicable set(s) of privacy principles.

Youth Partnerships is to be commended for its early assessment of privacy risk and proactive approach to privacy management. However, at this point, the key focus should be – and will remain for some time – undertaking foundational privacy work that will enable the *Youth*

Partnerships demonstration sites to proceed with confidence that privacy risks may be identified accurately and managed appropriately.

There are numerous options available to *Youth Partnerships* in terms of developing a strong privacy foundation. Based on the outcomes of the PIA process, including consultation with stakeholders, the following practical steps are recommended as a starting point.

Recommendation 2

It is considered that the primary privacy focus for *Youth Partnerships* at this point in time is to develop a strong privacy foundation capable of sustaining and guiding the activities of the seven demonstration sites operating under the *Youth Partnerships* umbrella.

It is recommended that *Youth Partnerships* takes the following practical steps towards achieving this aim:

1. Development of a shared set of *Youth Partnerships* privacy tenets to guide the demonstration sites as they engage with *Youth Partnerships;*
2. Development of a *Youth Partnerships* Privacy Management Framework to help the demonstration sites take a common approach to privacy management, including consistent documentation of key requirements (legislative, technical, policy, etc.) even as their various implementation activities diverge;
3. Incorporation of relevant privacy content into the *Youth Partnerships* Common Practice Framework; and
4. Provision of coordinated privacy training across the seven demonstration sites.

Youth Partnerships – Privacy Environment

Background

'Privacy' is a highly contested term, producing a bewildering range of definitions and philosophical, technical and legal accounts. One of the most enduring privacy definitions states that privacy is the right 'to be let alone'.[14] But, despite its appeal and simplicity, this definition does not provide clarity in terms of privacy obligations and responsibilities.

More recently, it has become popular to divide privacy into four main sub-categories as a means of increasing clarity:[15]

- **Information privacy**, which involves the establishment of rules governing the collection and handling of personal data such as credit information, and medical and government records. It is also known as 'data protection';
- **Bodily privacy**, which concerns the protection of people's physical selves against invasive procedures such as genetic tests, drug testing and cavity searches;
- **Privacy of communications**, which covers the security and privacy of mail, telephones, e-mail and other forms of communication; and
- **Territorial privacy**, which concerns the setting of limits on intrusion into the domestic and other environments such as the workplace or public space. This includes searches, video surveillance and ID checks.

When 'privacy' is raised in the context of *Youth Partnerships,* it refers to the specific subset 'information privacy' or 'data protection' and is concerned with the collection and handling of personal information. Information privacy laws are designed to provide a legislative framework for the responsible collection and handling of personal information. These laws are ordinarily based upon a set of information privacy principles that seek to maximise an individual's control over his or her own personal information, at the same time ensuring that organisations follow a minimum set of privacy standards.

Australia's federal system has produced a 'patchwork' of privacy protection comprising an overlapping and incomplete set of Commonwealth, State and Territory privacy laws. This privacy patchwork ratchets up the degree of privacy complexity as, depending on the nature of the organisation and its location, as well as the type(s) of personal information involved, different privacy laws may come into play. In some cases, multiple information privacy laws – each with its own set of privacy principles – may apply to a single organisation.

The Australian Law Reform Commission (ALRC) concluded a major review of Australian privacy law and practice in 2008.[16] It recommended the streamlining and reform of Australia's

[14] Samuel Warren and Louis D Brandeis, *The Right to Privacy*, originally published in 4 Harvard Law Review 193 (1890), http://www.louisville.edu/library/law/brandeis/privacy.html.
[15] D Banisar, *Privacy and Human Rights 2000: An International Survey of Privacy Law and Developments* Privacy International, http://www.privacyinternational.org/survey/phr2000/overview.html, cited by the Australian Law Reform Commission (ALRC) in its monumental review of Australian privacy law and practice, *For Your Information: Australian Privacy Law and Practice,* Report 108 (May 2008), Volume 1, p.142.
[16] ALRC, *For Your Information: Australian Privacy Law and Practice,* Report 108 (May 2008): http://www.alrc.gov.au/publications/report-108.

patchwork approach to privacy protection. In its response, the Australian Government supported reform, including the development of a single set of privacy principles.[17] However, to date, no legislative reform has been effected and it is unlikely that widespread, national reform will occur during the life of *Youth Partnerships*.

Privacy in Victoria

Victoria has two major information privacy laws: the *Information Privacy Act 2000* (IPA) and the *Health Records Act 2001* (HRA). The IPA was enacted in 2000 and contains ten Information Privacy Principles (IPPs), which provide the framework for information privacy management in the Victorian public sector. The HRA was enacted in 2001 and contains eleven Health Privacy Principles (HPPs), which provide the framework for health information privacy management in the public and private sectors in Victoria.[18]

In addition to the primary information privacy laws, further references to privacy are found in the *Charter of Human Rights and Responsibilities Act 2006* (the Charter).

Key Definitions

In Victoria personal information is defined as:

> [I]nformation or an opinion (including information or an opinion forming part of a database), that is recorded in any form and whether true or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

The IPA also provides special recognition to a subset of personal information defined as 'sensitive'. This includes information relating to race, sexuality, criminal history and religion. Collection, use and disclosure of such data will ordinarily require consent.

In Victoria, health information is defined in the HRA as:

> (a) information or an opinion about –
>
> (i) the physical, mental or psychological health (at any time) of an individual; or
>
> (ii) a disability (at any time) of an individual; or
>
> (iii) an individual's expressed wishes about the future provision of health services to him or her; or
>
> (iv) a health service provided, or to be provided, to an individual- that is also personal information; or
>
> (b) other personal information collected to provide, or in providing, a health service; or … but does not include health information, or a class of health information or health information contained in a class of documents, that is prescribed as exempt health information for the purposes of the *Health Records Act 2001* generally or for the

[17] Department of Prime Minister & Cabinet, *Privacy Reforms*, First Stage Response – Exposure Draft Legislation: http://www.dpmc.gov.au/privacy/reforms.cfm.

[18] Additionally, the IPA establishes the Office of the Victorian Privacy Commissioner (OVPC), which, in turn, oversights the IPA. The OVPC has a number of functions, including receipt, investigation and conciliation of complaints. However, responsibility for discharging information privacy requirements under the IPA resides with the relevant public sector organisation. The Victorian Health Services Commissioner administers the HRA and, likewise, may receive, investigate and conciliate complaints. Again, responsibility for discharging privacy requirements under the HRA resides with the relevant public sector organisation. Full copies of the IPA and HRA are available at http://www.legislation.vic.gov.au.

purposes of specified provisions of the *Health Records Act 2001.*

Like sensitive information, consent is a key precondition to collecting, using and disclosing health information. (The other precondition is that the information is necessary for a legitimate function or activity.)

As a corollary, privacy legislation *does not apply* to information that is de-identified or non-identifiable. However, whenever de-identified data has been derived from identifying or identifiable data caution must be exercised, as the data may be re-identifiable under certain circumstances. If data is re-identifiable it remains within the purview of privacy legislation.

Application

On the whole, the IPA and the HRA operate concurrently with a wide range of other Victorian statutes, including the *Children, Youth and Families Act 2005* (Vic) and the *Mental Health Act 1986* (Vic). However, in the case of any inconsistency between privacy legislation and other, governing legislation, privacy requirements give way to the degree of any inconsistency.[19] If specific authorisations relating to the collection and handling of personal information are contained in governing legislation, the IPA recognises that these are 'authorised by law' and take precedence over the requirements of the IPPs. So too, if prohibitions exist – such as confidentiality provisions – they override more flexible or facilitative provisions contained in the IPPs (or, in the case of health information, the HPPs).

The IPA and HRA cover Victorian public sector organisations like DEECD, the Department of Health, local government and Victoria Police whenever they collect and handle personal information, including sensitive and health information. Each organisation is responsible for its own privacy compliance even when involved in a WOVG initiative. In certain instances, the IPA may also extend to private sector organisations providing youth services.

Victorian privacy laws contain an outsourcing mechanism that enables Victorian public sector privacy requirements to extend to Victorian contracted service providers *as if they were* Victorian public sector organisations as long as a suitable privacy clause is included in the services contract or funding agreement. Victorian public sector organisations incorporate such clauses into funding agreements and contracts for service delivery as a matter of course. Thus, the IPA may cover private sector youth services organisations that would otherwise be covered by federal privacy legislation when they provide youth services on behalf of the Victorian Government.

Privacy Act 1988 (Cth)

The federal *Privacy Act 1988* (Cth) applies to Commonwealth and ACT public sector organisations and establishes Information Privacy Principles (IPPs) that apply to personal information, including health information, collected and handled by the public sector.

In 2001, the Privacy Act was extended to parts of the Australian private sector – including not-for-profit entities operating in the youth services field – which must comply with a set of National Privacy Principles (NPPs). The federal Privacy Act covers both personal and health information; there is no separate regime for health information at the federal level. Health information is grouped with other 'sensitive' personal information and subject to greater protection.

[19] Privacy legislation is not absolute. It recognises information privacy as an important public interest that may require balancing against other public interests, including.

As with the operation of Victorian privacy law, the Privacy Act operates concurrently with a wide range of other Commonwealth statutes. Again, in the case of any inconsistency between privacy legislation and other, governing legislation, privacy requirements give way to the degree of inconsistency. Like Victorian privacy legislation, the Privacy Act contains an outsourcing mechanism that may extend federal public sector privacy requirements to private sector organisations that would otherwise be exempt (e.g. small businesses). This is achieved via a privacy clause requiring private sector organisations to comply with the public sector IPPs as well as the four NPPs that are not covered under the IPPs.[20]

Managing Regulatory Complexity

In a multi-party environment like *Youth Partnerships* additional complexity in relation to privacy obligations arises on at least three levels:

1. The impact of multiple privacy laws (which may operate concurrently but contain different sets of privacy principles);
2. The impact of governing legislation (which may impose different information collection and handling requirements to those found in privacy laws); and
3. The impact of funding agreements that incorporate a privacy clause (which may displace one set of privacy principles for another under certain circumstances).

The Privacy Patchwork

While *Youth Partnerships* is a WOVG initiative and subject to Victorian privacy legislation, it does not 'cover the field' in relation to participants' privacy compliance obligations.

Victorian public sector organisations participating in *Youth Partnerships* are subject to the IPA and HRA and must comply with the Victorian IPPs and HPPs respectively. Not-for-profit organisations are subject to the private sector provisions of the federal Privacy Act and must comply with the NPPs. As privacy obligations apply at an organisational level, this means that a variety of privacy policies will be in place across the *Youth Partnerships* environment.

Providing participants with explanatory, high-level information about the privacy patchwork will help to minimise any concerns about differences in privacy compliance measures. In particular, it may be beneficial to explain to participants that:

- The same basic privacy requirements are common to the various legislative privacy schemes; and
- *Youth Partnerships* is committed to developing an overarching approach to privacy that is designed to leverage this commonality and provide a holistic privacy management framework.

Recommendation 3

It is recommended that explanatory, high-level information about the Australian 'privacy patchwork' and its impact is provided in the Common Practice Framework.

More detailed information about the approach to managing this patchwork may be provided via the *Youth Partnerships* website.

[20] That is: NPP 7 – Government Identifiers, NPP 8 – Anonymity, NPP 9 – Transborder Data Flows and NPP 10 – Sensitive Information

'Overriding' Privacy

As part of the preliminary privacy survey, the demonstration sites were asked to identify all applicable *Youth Partnerships* legislation, not just privacy legislation. The list provided references more than twenty separate statutes, excluding the IPA, HRA and Privacy Act. (See Appendix A.) While not all of these laws impact on the collection and handling of personal information, a significant number do. In certain circumstances they may also override privacy requirements.

The *Youth Partnerships* regulatory framework is, therefore, quite 'crowded'. As privacy legislation is subordinate to other, more specific governing legislation to the degree of any inconsistency, this means that if another law imposes a specific obligation or requirement in relation to the collection and/or handling of personal information in the *Youth Partnerships* context, this will provide the legal framework, not privacy. This 'privacy override' mechanism is a source of considerable confusion if not managed effectively.

It must be acknowledged that each of the organisations involved in *Youth Partnerships* is *already* working in this environment. In this sense, *Youth Partnerships* is not creating a new set of issues, rather the increased focus on information sharing creates more awareness of the potential 'to get this wrong', at times resulting in risk-averse behaviour.

One of the best ways to tackle this problem is to address it head on: acknowledging the issue, identifying key instances of the privacy override in operation and providing practical examples of when it occurs and how to manage it.

Recommendation 4

It is recommended that steps be taken to identify and document the main instances of 'privacy override' that will occur in the *Youth Partnerships* context to inform participants about their impact.

While the Common Practice Framework is not a suitable home for such detailed privacy information, it is considered that relevant information may be provided at a detailed level via the *Youth Partnerships* website (under a privacy management heading).

Funding Agreements and Privacy Clauses

As outlined above, section 3.4.1, a single organisation participating in *Youth Partnerships* may be subject to multiple sets of privacy principles because of the privacy patchwork. However, this may become even more complex in the context of funding agreements.

Many of the organisations involved in *Youth Partnerships* receive both Victorian and federal funding. Each funding agreement will incorporate a privacy clause that imposes the funder's privacy obligations upon the contracted service provider. This may result in the displacement of the primary set(s) of privacy principles with another set of privacy principles and an increased privacy compliance burden, as organisations are required to comply with multiple privacy principles.

The following case study, identified during the PIA process, provides an illustration of the way in which a funding agreement may impact upon privacy compliance requirements.

Case Study

A not-for-profit organisation participating in *Youth Partnerships* provides a centralised referral service to young people. This organisation routinely utilises up to five different consent forms at the *beginning* of the engagement process.

An initial consent form covers the centralised referral process.

Following the referral intake assessment, a young person may be given an internal or external referral, depending on the specific circumstances and needs of the young person.

If the referral is internal, one of four different consent forms is then utilised depending on the source of funding (i.e. particular program) and the requirements attached to that funding (e.g. extension of federal or Victorian public sector privacy principles and/or specific reporting obligations).

Comments

The existence of multiple consent forms within a single organisation, for ostensibly the same services, arises as a direct result of the privacy patchwork and the outsourcing provisions contained within the various privacy laws that extend the funding organisation's privacy obligations to the contracted service provider.

From a privacy perspective, it is difficult to see how five separate consent forms benefit an individual young person seeking assistance.

From the perspective of youth services workers, the existence of multiple consent forms is likely to be viewed as a form of risk management on the part of the funding organisation rather than a genuine concern to ensure that individual young people are fully informed about privacy.

The challenge for *Youth Partnerships* is to try and ensure that participation in *Youth Partnerships* does not result in an additional privacy compliance burden except where necessary and desirable.

Youth Partnerships' participants do not need to understand the detail and consequences of the various privacy laws' outsourcing mechanisms. From a practical perspective, however, it may be advantageous for *Youth Partnerships'* privacy materials to articulate an approach to privacy that is broadly compatible with all relevant privacy principles, reflecting the need to accommodate the competing privacy regimes imposed under a range of funding agreements.

While the various sets of privacy principles in place across Australia are not identical, they do share a common antecedent in the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*.[21] Further, the Victorian IPPs and HPPs are based on the

[21] Organisation for Economic and Co-operation and Development (OECD), *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980). See, too, OECD, *The Evolving Privacy Landscape: 30 Years after the OECD Privacy Guidelines* (April 2011).

private sector NPPs, mirroring their structure and containing much content in common. In recognition of the varying impact of funding arrangements upon privacy compliance, it is considered beneficial for *Youth Partnerships* to account for privacy principles at both a generic level (via the Common Practice Framework) and a specific level (via detailed information published on the *Youth Partnerships* website).

Recommendation 5

It is recommended that the privacy information developed for the *Youth Partnerships* Common Practice Framework take a 'highest common denominator' approach to privacy principles, providing a generic account of the privacy principles that is designed to increase knowledge about the information lifecycle enshrined within the privacy principles rather than describing the specific detail of, for example, the Victorian IPPs or HPPs.

In due course, participants should be provided with more detailed information about the specific privacy principles applicable to *Youth Partnerships* as a WOVG initiative via the *Youth Partnerships* website.

Youth Partnerships Information Flows

Accounting for the Privacy Principles – the Information Lifecycle

Privacy principles are not prescriptive, they do not tell you what to do, rather they provide a framework for the responsible collection and handling of personal information. Privacy principles need to be applied to a given fact situation and require a degree of 'thought' in order to produce a good 'judgement'. This makes it difficult to provide definitive advice in the abstract, particularly in the absence of specific details about an initiative.

Privacy principles are based upon the notion of an 'information lifecycle' in which the entire lifecycle of personal information from collection through to archiving and destruction is the subject of assessment. It is important that stakeholders understand – broadly – the information lifecycle addressed by the privacy principles, encompassing each principle's individual content as well as the way they overlap and interconnect with each other.

Awareness of the privacy principles' information lifecycle will help ensure that *Youth Partnerships* is consistent with privacy requirements. By way of example, the following diagram illustrates, at a high level, the interconnected nature of the privacy principles.[22]

[22] This diagram is adapted from the Office of the Victorian Privacy Commissioner's *Guidelines to the Information Privacy Principles* (edition 3) November 2011, p.2: http://www.privacy.vic.gov.au/privacy/web2.nsf/files/guidelines-to-the-information-privacy-principles/$file/guideline_11_11.pdf.

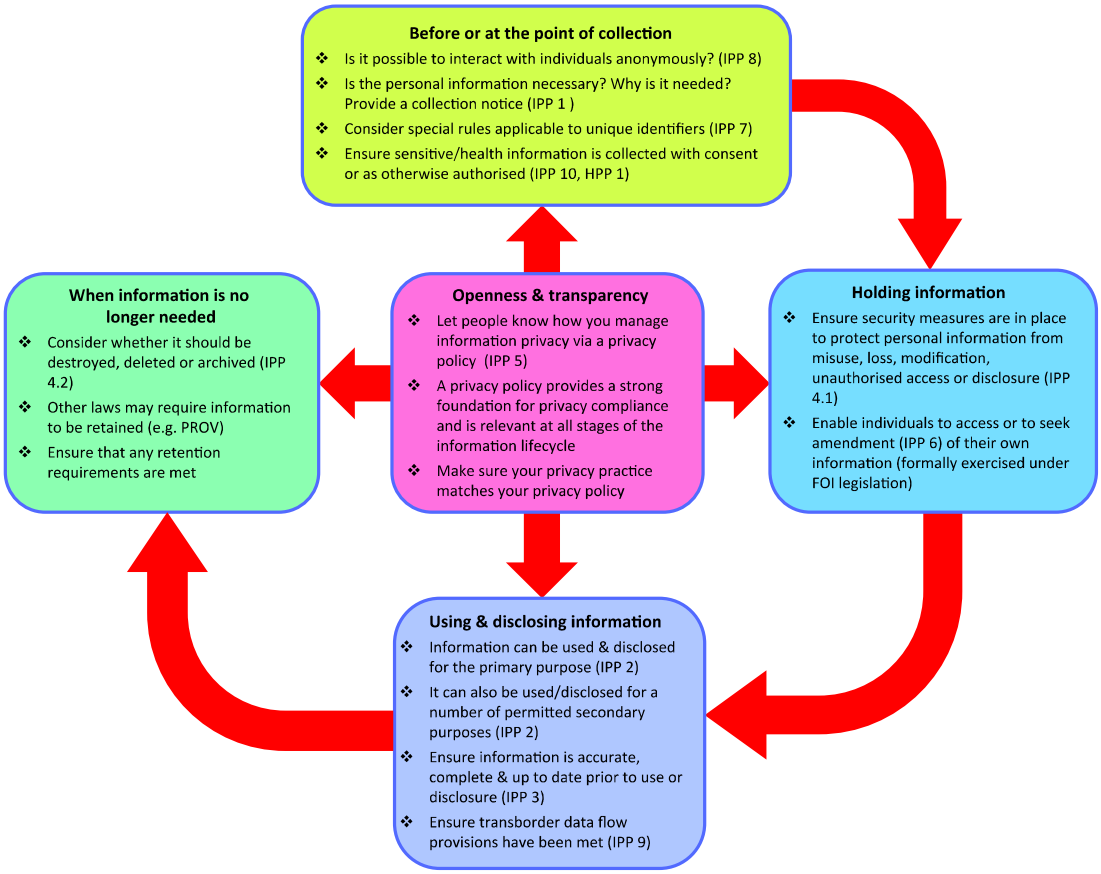


Figure 1 – Information Lifecycle – Applying the IPPs

The objects of privacy legislation also need to be taken into account when applying privacy principles. For example, the IPA has three objects:

- To balance the public interest in the free flow of information with the public interest in protecting the privacy of personal information in the public sector;
- To promote awareness of responsible personal information handling practices in the public sector; and
- To promote the responsible and transparent handling of personal information handling in the public sector.[23]

It is surprising how little awareness there is of the first of these three objects. Reflecting the influence of the OECD Guidelines, the first object notes the importance of seeking to balance two important public interests – privacy *and* the free flow of information. As a starting point, this means that it is legitimate to consider ways of promoting better ways of providing youth services, including through improved information sharing. The key is to seek to achieve this goal in a way that is consistent with the requirements of the IPPs.

[23] Section 5, *Information Privacy Act 2000* (Vic).

An Overview of Privacy Principles

There are examples of generic or common privacy principles available that may be used by *Youth Partnerships*.[24] However, for the purposes of the PIA report a short summary of 'Privacy Principles' is provided below for illustration purposes.

Privacy Principle	Meaning & General Compliance Requirements
1. Collection	*The Collection principle is critical to overall privacy compliance. If the initial collection requirements are managed well, it is likely to result in compliance with other privacy principles. To the degree that collection is not well managed, it will invariably lead to problems downstream.* *The Collection principle requires organisations to take a number of steps to ensure that any collection of personal information is:* • *Necessary and proportional;* • *Consistent with the organisation's functions and activities;* • *Conducted by lawful and fair means;* • *Collected directly from the individual where possible; and* • *Subject to notice* *'Notice' refers to the requirement that individuals are provided with information about:* • *The identity of the organisation collecting the information and how to contact it;* • *The fact that individuals may gain access to their own information;* • *The purposes for which the information is collected;* • *To whom the organisation usually discloses information of that kind;* • *Any law that requires the particular information to be collected; and* • *The main consequences (if any) for the information if the information is not provided.* *Personal information defined as 'sensitive' or 'health' information must also be collected with consent (see 10. Sensitive/Health Information, below).*
2. Use & Disclosure	*The Use and Disclosure principle is a purpose-limitation principle.* *The Use and Disclosure principle provides that:* • *Personal information may be used and disclosed for the primary purpose for which it was collected.* • *Personal information may be used or disclosed for a related secondary purpose that an individual would reasonably expect (directly related in the case of sensitive or health information).* • *Other uses and disclosures should operate on the basis of consent or*

[24] See, for example, the following resources available via the OVPC website: *Comparative Table of Privacy Principles* (September 2002), *IPPs in everyday language* (May 2002) and *Information Privacy Principles,* www.privacy.vic.gov.au.

	as authorised by law. • *Additional specified exceptions may apply on a case-by-case basis, e.g. for research, quality assurance, public safety or law enforcement purposes.*
3. Data Quality	*The Data Quality principle aims to ensure that personal information is subject to a degree of quality assurance.* *Reasonable steps must be taken to ensure that personal information is accurate, complete and up to date, particularly in relation to its use and disclosure.*
4. Data Security	*The Data Security principle is designed to protect personal information from misuse, unauthorised access, modification or disclosure. It applies regardless of whether the information is held in electronic or hard copy format. It is concerned with three categories of security: IT/logical, physical and personnel.* *This principle also requires that information be destroyed or disposed of appropriately if it is no longer needed and must be interpreted in the context of any requirements imposed by the public records legislation (in the case of public sector records) or other legislation requiring or specifying periods of retention of information.*
5. Openness	*The Openness principle is a critical foundation stone for general privacy compliance as well as a clear demonstration of an organisation's awareness of, and commitment to, the responsible collection and handling of personal information (including health and sensitive information).* *It requires that organisations have clearly expressed policies on their management of personal information and that the information is readily available should anyone ask for it.*
6. Access & Correction	*The Access and Correction principle is designed to provide individuals with a statutory right to seek access to (and alteration/correction of) personal information about them.* *Organisations must comply with a number of requirements relating to the provision of access and correction.* *In the public sector, this principle overlaps with access regimes established under Freedom of Information (FOI) legislation (which provides a statutory right for individuals to seek access to government information, including information about themselves). FOI legislation provides the mechanism for access/correction requests in the public sector.*
7. Unique Identifiers	*The Unique Identifiers principle addresses potential privacy issues associated with the use of unique identifiers, particularly where issued by government.* *Unique identifiers are useful for managing interactions with large numbers of people as well as for authentication purposes. However, identifiers also have the capacity to enhance data matching and encourage 'information or function creep'.* *This principle limits the capacity for unique identifiers to be adopted and shared across and beyond government by imposing a number of requirements*

	and limitations on their adoption and use.
8. Anonymity	*The Anonymity principle is designed to promote the ability of people to interact with organisations – including government organisations – without identifying themselves.* *This principle requires that organisations take reasonable steps to provide individuals with anonymous means of interacting with them wherever practicable.*
9. Transborder Data Flows	*The Transborder Data Flows principle is designed to address issues raised by the transfer of personal information beyond jurisdictional boundaries and the reach of local privacy legislation.* *In particular, it aims to prevent situations where the transfer of personal information across borders (state, national) will result in the loss of legislative protection for privacy.*
10. Sensitive/Health Information	*Additional protection is provided to personal information defined as 'sensitive' under IPA. This includes information about an individual's sexuality, race, trade union membership and religion. Health information is another form of sensitive information and, in Victoria, is subject to additional protection under the HRA.* *As a starting point, any collection of sensitive of health information must be both necessary to the exercise of an organisation's legitimate function/activity and subject to consent. Limited exceptions may be available under certain circumstances.*

Youth Partnerships Information Flows

Youth Partnerships involves personal information about individual young people (including health and sensitive personal information) being collected and handled by organisations involved in the *Youth Partnerships* demonstration sites – subject to a young person's consent – in order to provide more coordinated youth services. *Youth Partnerships* is committed to a consent-based, young-person centred, model of care.

As noted previously, the PIA found that:

- *Youth Partnerships* is not a specific initiative *per se*, rather it is a framework within which a number of independent implementation sites will seek to develop better, more coordinated ways of providing youth services. There is no single approach to the delivery of *Youth Partnerships*. Rather, each demonstration site is able to develop its own approach, based on local needs and service delivery infrastructure; and
- *Youth Partnerships* is not sufficiently advanced to undertake a comprehensive PIA at this point in time (either at the level of *Youth Partnerships* or at the level of an individual demonstration site). Therefore, it is not possible to account for *Youth Partnerships* 'end-to-end' and from a 'whole-of-information-lifecycle' perspective. In practical terms this means that it is not possible to map information flows of personal information against the requirements of the relevant sets of privacy principles;

While it is not possible to conduct a fully-fledged mapping of privacy principles at this point in time, it has been possible to put together an individual *Youth Partnerships* demonstration site

‘case scenario’ and provide a high-level assessment of it in terms of information flows and privacy requirements. (See Appendix B – Youth Partnerships Information Flows)

Managing Privacy across *Youth Partnerships*

Youth Partnerships is a WOVG initiative involving multiple organisations that will be implemented across multiple demonstration sites. The overarching privacy objective is to achieve a holistic approach to privacy across each of the seven demonstration sites, while at the same time enabling each demonstration site to pursue the best set of implementation activities based on location, resources and individual circumstances.

In a practical sense, each organisation participating in a demonstration site will remain responsible for its own privacy compliance program. However, in order to achieve the best set of outcomes for *Youth Partnerships* (both in terms of policy outcomes and privacy protection), it is also necessary to ensure that each participating organisation and its employees understands the approach taken at a *whole-of-initiative* level.

The PIA has identified that the first priority for *Youth Partnerships* is to develop a strong privacy foundation, comprising a purpose-built approach to privacy that is capable of protecting and managing privacy – at a whole of initiative level – over time. This approach also needs to be communicated to all stakeholders and participants.

There are numerous privacy management options available to *Youth Partnerships*. Based on the PIA process, a suggested 'short list' of privacy strategies has been recommended in this report and addressed in this chapter. However, it is noted that these are not mandatory, and it is open to *Youth Partnerships* to develop an alternative set of strategies. The critical point is to ensure that there is a clearly articulated approach to privacy, designed to maximise privacy compliance and promote effective privacy practices.

The specific privacy management elements identified during the *Youth Partnerships* PIA are:

- *Youth Partnerships* Common Practice Framework
- *Youth Partnerships* Privacy Management Framework
- *Youth Partnerships* Privacy Tenets

Common Practice Framework

A key theme arising from the *Youth Partnerships* PIA is the importance of 'operationalising' privacy. If privacy becomes part of everyday practice, there is less risk of it being viewed as 'special' or 'difficult'. As an initial step, incorporating privacy content into the Common Practice Framework is preferable to developing a stand-alone *Youth Partnerships* privacy manual or privacy policy. By making a recommendation to incorporate privacy content into the Common Practice Framework, this report confirms the approach initially identified by the *Youth Partnerships* Secretariat when it commissioned the PIA.

Developed by the *Youth Partnerships* secretariat, the Common Practice Framework aims to support a common language, understanding and evidence-based practice across *Youth Partnerships.* It articulates overarching principles relevant to the provision of more coordinated youth services that may be shared by all stakeholders.

The Common Practice Framework provides an opportunity to incorporate privacy content into a generic *Youth Partnerships* guide. As the scope of the framework's privacy content is necessarily limited, it should focus on providing a positive, high-level introduction to privacy in the context of *Youth Partnerships* rather than seeking to develop a comprehensive account of

privacy. However, while the *amount* of privacy content that may be accommodated in the Common Practice Framework is restricted, it is nevertheless feasible and desirable that additional, more detailed, privacy content is developed and published/made available to stakeholders over time.

Common Practice Framework privacy content

Privacy content for the Common Practice Framework should be developed as a matter of priority, drawing upon the findings of the *Youth Partnerships* PIA.

The privacy content for the Common Practice Framework may consist of the following:

1. A positive statement to the effect that:
    - The aims of the *Youth Partnerships* initiative are consistent with all relevant privacy requirements;
    - A commitment to good privacy practice will enhance *Youth Partnerships,* not impede it; and
    - Privacy has been built into *Youth Partnerships* through the development of a strong privacy foundation. This foundation is based upon respect for individual privacy and is designed to help to minimise any risk of privacy breach and to promote positive privacy outcomes.
2. A brief summary of relevant Victorian and Commonwealth privacy legislation and compliance requirements
3. A brief summary of the *Youth Partnerships* approach to privacy (privacy foundation). This may include reference to *Youth Partnerships'* privacy tenets, *Youth Partnerships* privacy policy, *Youth Partnerships* Privacy Management Framework and the delivery of privacy training.

Additional Privacy Content – Youth Partnerships Website

A *Youth Partnerships* website is currently being developed. It is considered that the website may provide a suitable home for more detailed privacy content (accessed directly via the website and/or through links within the Common Practice Framework itself) as well as providing external links to other relevant privacy information (e.g. online information provided by the Office of the Victorian Privacy Commissioner and the Victorian Office of the Health Services Commissioner).

While the development of additional privacy material is subordinate to the need to develop and finalise privacy content for the Common Practice Framework, it is recommended that additional privacy material be developed in the future.

This could include operational guidance for *Youth Partnerships* stakeholders in relation to their privacy obligations, including discussion of common privacy issues and illustrative case studies as well as providing a home for generic privacy forms, policies and protocols.

In light of the complex regulatory environment, any expanded privacy content will need to be subject to quality control, particularly in relation to specific professional requirements that may impact upon otherwise standard interpretations or applications of privacy legislation and practice.

Youth Partnerships Privacy Tenets

One of the PIA's key findings is that it would be beneficial for a set of privacy tenets to be developed for *Youth Partnerships.* In an environment in which up to four separate sets of privacy principles may apply to a participating organisation, a set of privacy tenets has the potential to provide a succinct, generic account of privacy that is readily understood and supported by stakeholders. It also clearly demonstrates *Youth Partnerships'* commitment to privacy.

Participants at the *Youth Partnerships* PIA Workshop, held on 8 December 2011, supported the development of a set of *Youth Partnerships* Privacy Tenets, applicable to *Youth Partnerships* as a whole.

Finalising privacy tenets for *Youth Partnerships* will require consultation and input from a range of key stakeholders. Draft text has been included in the PIA report to facilitate this consultation process.[25] It provides a basis for discussion only; it is not suitable for adoption in its current format.

Any *Youth Partnerships* privacy tenets should be drafted in clear, non-technical language, seeking to capture the core privacy requirements that *Youth Partnerships* needs to address.

***Youth Partnerships* – Draft Privacy Tenets (for discussion purposes only)**	
1.	**Commitment to Privacy** *Youth Partnerships'* stakeholders and participants are committed to protecting the privacy of individuals taking part in the *Youth Partnerships* initiative. It is recognised that privacy is integral to the success of *Youth Partnerships*. Wherever possible, *Youth Partnerships* will seek to promote privacy-positive outcomes. As part of this commitment to privacy, appropriate privacy resources and training will made available across the scheme. A strong privacy foundation will support the individual demonstration sites as they implement *Youth Partnerships.*
2.	**Youth-Centred Focus** *Youth Partnerships* is a consent-based, youth-centred initiative designed to improve the support offered to individual young people through enhanced information sharing and collaboration. *Youth Partnerships* will seek to ensure that any activities undertaken for *Youth Partnerships* are youth centred, based on consent and undertaken transparently and with respect.
3.	**Individual Participation**

[25] The draft *Youth Partnerships* Privacy Tenets are based upon a set of privacy tenets developed in the national eHealth context. See, *NEHTA's Approach to Privacy* (July 2006), section 2.1, NEHTA Privacy Tenets. http://www.nehta.gov.au.

	Youth Partnerships will seek to maximise the degree of control young people may exercise over the collection and handling of their personal information as a result of participating in *Youth Partnerships.* The *Youth Partnerships* demonstration sites will adopt this principle when developing their work programs and implementation activities.

4.	**Clarity & Transparency of Purpose** *Youth Partnerships* is committed to clarity and transparency in relation to any collection and handling of personal information under its auspices. An account of the purposes for which personal information may be collected and handled under *Youth Partnerships* will be documented and made available to all stakeholders and participants.
5.	**Accountability** *Youth Partnerships* will ensure that appropriate governance arrangements are established so as to ensure that these privacy tenets are supported and progressed at the level of each individual *Youth Partnerships* demonstration site, from development through to implementation.

Youth Partnerships Privacy Management Framework

Developing privacy content for the Common Practice Framework privacy content and finalising *Youth Partnerships* privacy tenets is relatively straightforward, providing a good starting point for privacy management efforts. However, more detailed privacy management strategies are also required. In light of the focus upon individual demonstration sites, it is also considered desirable for *Youth Partnerships* to implement a broader ranging *Youth Partnerships* Privacy Management Framework.

A PMF provides organisations and sector-wide initiatives with a structured approach for the end-to-end and whole-of-life management of the privacy of personal/health information.[26] PIA guides and other privacy tools, including those developed by the various Australian privacy regulators, may supplement a PMF.

The aim of a PMF is to enable organisations and sector-wide initiatives to 'operationalise' privacy by embedding the appropriate responsibilities, actions, checks and balances within existing management and risk control functions and activities.

Ordinarily, a PMF covers the following categories:

- Governance and Management
- Information Lifecycle Management
- Risk Assessment and Management

[26] Developed by David Jonas, Convergence e-Business Solutions Pty Ltd, www.convergence.com.au.

- Systems
- Information Access Control and Security
- Personnel
- Legal
- Privacy Management
- Compliance/conformance/certification
- Tracking, Audit and Reporting
- Persistence Management

The details and benefits of a PMF were presented and discussed at the *Youth Partnerships* PIA workshop (December 2011). Participants were supportive of the development of a *Youth Partnerships*-tailored PMF. It was considered that a PMF provided a consistent, structured approach to privacy management that could be implemented across each of the demonstration sites. In particular, this was viewed as enabling the seven demonstration sites to implement different approaches to the delivery of more coordinated youth services, while sharing a basic privacy framework, vocabulary and templates for recording privacy-related information (e.g. governance and management, information lifecycle management, etc.).

If a further *Youth Partnerships* PIA is undertaken in the future, the PMF will help ensure that relevant and consistent information and materials are readily available.

Workshop participants indicated that they would like to receive further information about a PMF as part of the *Youth Partnerships* PIA Report. Following the PIA workshop, the primary author of the PMF materials, David Jonas, prepared a stand-alone PMF document. This document – *Privacy Management Framework and Supporting Checklists* – is provided as a separate attachment to this PIA Report. It is recommended that further consideration be given to adopting a streamlined version of the PMF for the *Youth Partnerships* initiative.

Final Comments

While *Youth Partnerships* is a WOVG initiative, DEECD has been assigned the role of lead agency and a whole-of-government *Youth Partnerships* Secretariat is located within DEECD. In a practical sense, privacy management will be coordinated from within DEECD/by the secretariat. As part of these arrangements it will be necessary to identify who is responsible for the ongoing management of privacy from a whole-of-*Youth Partnerships* perspective.

From a governance perspective, any *Youth Partnerships* privacy measures need to be subject to strategic oversight. The strategic level of governance involves high-level decision-making and planning in relation to an initiative, e.g. oversighting the development and implementation of policies, determining priorities and setting directions. The Children's Services Coordination Board undertakes the strategic governance role in relation to *Youth Partnerships.*

From a practical viewpoint, it is expected that the *Youth Partnerships* Secretariat will be responsible for progressing work on the privacy foundation in accordance with the board's instructions and in consultation with key stakeholders. Following receipt of the *Youth Partnerships* PIA report, the secretariat will need to develop a privacy work plan and associated timeframe for implementing the PIA's recommendations.

In terms of this PIA report, the process may be illustrated as follows:

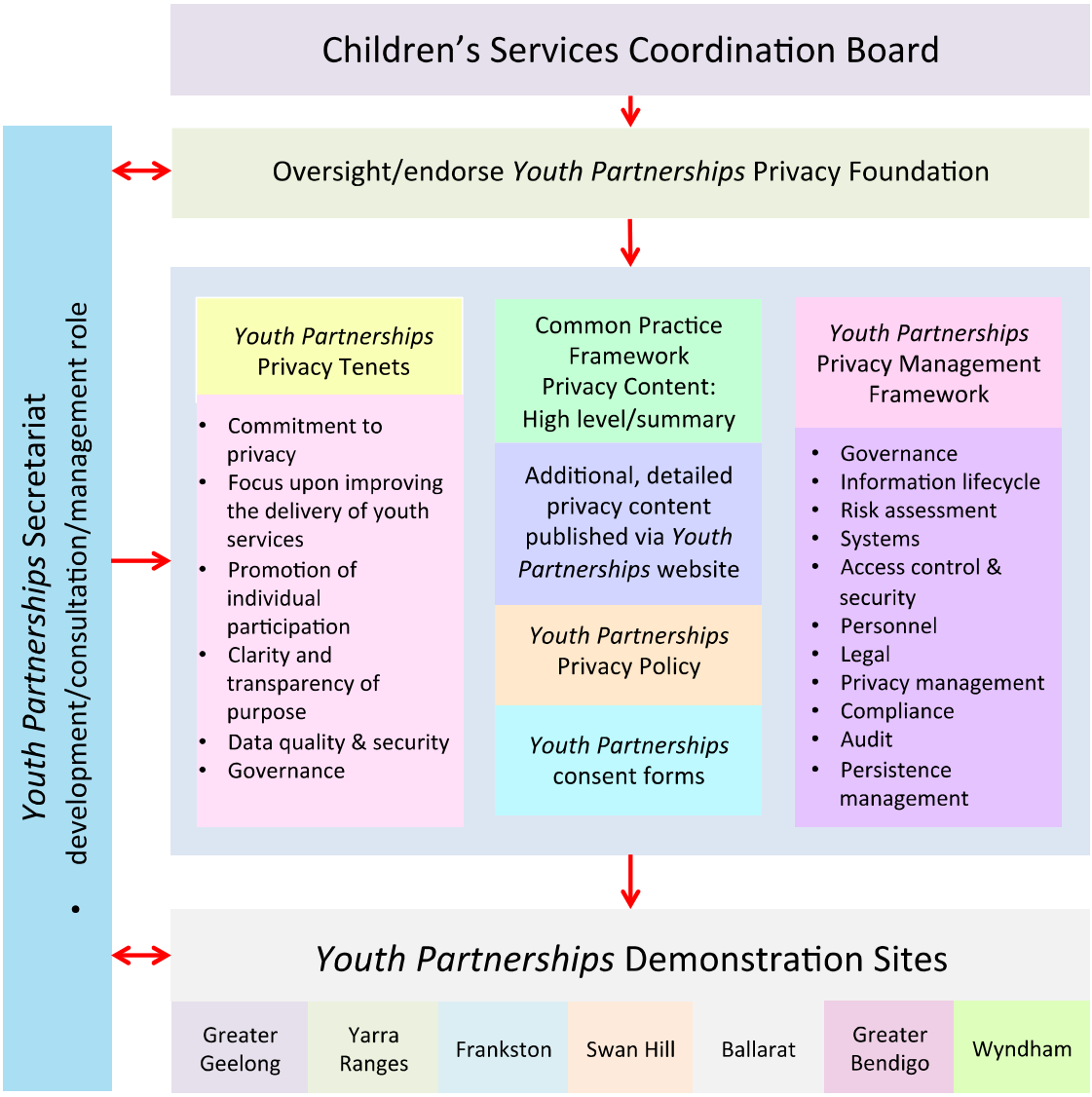


Figure 2 – Development of Youth Partnerships' Privacy Foundation

Glossary and acronyms

The Charter	*Charter of Human Rights and Responsibilities Act 2006 (Vic)*
Contracted service provider	A person or body providing services under a contract to a Victorian public sector organisation (the outsourcing organisation) in connection with the performance of functions of the outsourcing organisation, including services that the outsourcing organisation is to provide to other persons or bodies
DEECD	Department of Education and Early Childhood Development (Victoria)
DH	Department of Health (Victoria)
DHS	Department of Human Services (Victoria)
Health information	(a) information or an opinion about- (i) the physical, mental or psychological health (at any time) of an individual; or (ii) a disability (at any time) of an individual; or (iii) an individual's expressed wishes about the future provision of health services to him or her; or (iv) a health service provided, or to be provided, to an individual- that is also personal information; or (b) other personal information collected to provide, or in providing, a health service; or (c) other personal information about an individual collected in connection with the donation, or intended donation, by the individual of his or her body parts, organs or body substances; or (d) other personal information that is genetic information about an individual in a form which is or could be predictive of the health (at any time) of the individual or of any of his or her descendants; but does not include health information, or a class of health information or health information contained in a class of documents, that is prescribed as exempt health information for the purposes of the *Health Records Act 2001* generally or for the purposes of specified provisions of the *Health Records Act 2001*
HPPs	Health Privacy Principles
HRA	*Health Records Act 2001 (Vic)*
IPA	*Information Privacy Act 2000 (Vic)*
IPPs	Information Privacy Principles
NPPs	National Privacy Principles

OHSC	Office of the Health Services Commissioner
OVPC	Office of the Victorian Privacy Commissioner
personal information	Information or an opinion (including information or an opinion forming part of a database), that is recorded in any form and whether true or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion, but does not include information of a kind to which the *Health Records Act* applies
PIA	Privacy Impact Assessment
PMF	Privacy Management Framework
Privacy Act	*Privacy Act 1988 (Cth)*
sensitive information	Personal information that is also about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual preferences or practices, or criminal record
unique identifier	an identifier (usually a number) assigned by an organisation to an individual uniquely to identify that individual for the purposes of the operations of the organisation but does not include an identifier that consists only of the individual's name but does not include an identifier within the meaning of the *Health Records Act*

Appendix A – Legislation relevant to *Youth Partnerships*[27]

Privacy Legislation

Information Privacy Act 2000 (Vic)

Health Records Act 2001 (Vic)

Privacy Act 1988 (Cth)

Governing Legislation

Mental Health Act 1986 (Vic)

Severe Substance Dependence Treatment Act 2010 (Vic)

Anglican Welfare Agency Act 1997 (Vic)

Victorian Curriculum and Assessment Authority Act 2000 (Vic)

Charter of Human Rights and Responsibilities Act 2006 (Vic)

Child Wellbeing and Safety Act 2005 (Vic)

Children's Services Act 1996 (Vic)

Children, Youth and Families Act 2005 (Vic)

Commonwealth Powers (Family Law-Children) Act 1986 (Cth)

Criminal Procedure Act 2009 (Vic)

Drugs, Poisons and Controlled Substances Act 1981 (Vic)

Education and Training Reform Act 2006 (Vic)

Family Violence Protection Act 2008 (Vic)

Freedom of Information Act 1982 (Vic)

Guardianship and Administration Act 1986 (Vic)

Health Professions Registration Act 2005 (Vic)

Housing Act 1983 (Vic)

Human Services (Complex Needs) Act 2009 (Vic)

Legal Aid Act 1978 (Vic)

Local Government Act 1989 (Vic)

Magistrates' Court Act 1989 (Vic)

Parole Orders (Transfer) Act 1983 (Vic)

[27] This list of legislation was developed as part of the preliminary PIA privacy survey. It is not considered to be a complete list of applicable legislation but, rather, is intended to provide an indication of the breadth of the legislative environment that *Youth Partnerships* operates within.

Public Administration Act 2004 (Vic)

Public Records Act 1973 (Vic)

Residential Tenancies Act 1997 (Vic)

Appendix B – *Youth Partnerships* Information Flows Scenario

Sample Youth Partnerships Demonstration Site Case Scenario

Spencer lives with a carer in the Central Highlands region of Victoria. His legal Guardian is the State of Victoria. Throughout his life, Spencer has suffered significant trauma. His mother is a drug addict, and also has mental health issues. His father committed suicide in front of Spencer when he was six years old. He is now fifteen years old and has not attended school since grade five.

A local Education Alliance Coordinator has recently been employed by the Youth Partnerships Demonstration Site Governance Committee to undertake coordination activities across the Youth Partnerships Demonstration Site.'

The Education Alliance Coordinator has referred Spencer to the local Youth Partnerships Agency Support Team. The purpose of the referral is for the team to identify options to provide a more coordinated and targeted set of services to Spencer.

Prior to the referral, the Education Alliance Coordinator sought and gained informed consent from Spencer and from his carer to participate in the Youth Partnerships Demonstration Site. As part of the consent process, Spencer and his carer have both signed Youth Partnerships consent forms. The consent form includes information about the purpose of Youth Partnerships (i.e. to support the delivery of coordinated youth services), outlines how Spencer's personal information will be collected and handled under Youth Partnerships as well as listing the various organisations participating in the Youth Partnerships Agency Support Team.

The Education Alliance Coordinator has scheduled the first Youth Partnerships Agency Support team meeting to discuss how the group may collectively advocate for Spencer. Represented at the meeting is the local Human Development worker, the Central Highlands Family Services Coordinator, the Central Highlands Health Centre Coordinator and the Neighbourhood Centre Coordinator.

The Education Alliance Coordinator asks each of the participants to outline how they have been involved with Spencer previously and to discuss what they can achieve collectively to put in place a clear and coordinated pathway for Spencer.

It soon emerges that each participant has an entirely different view of what is meant by privacy. As various perspectives on what privacy means for each organisation emerge, these impact on the discussions that are meant to help Spencer. Issues are raised around what is meant by informed consent? Who is the referring agency? Have they consulted with each of the other agencies? Has each agency been 'cleared' by its management to enter into this new way of working? Which agency's privacy policy will apply to this situation? Does one privacy policy prevail over other policies? Does a Youth Partnerships privacy policy need to be written? Will each agency contravene privacy legislation if it participates in the meeting?

Mapping of Privacy Principles

The case scenario describes a situation in which a young person and his carer have been informed about the local *Youth Partnerships* demonstration site.[28] We are told that informed consent has been sought from Spencer and his carer for Spencer to participate in the identification of options for a more coordinated and targeted set of services. This results in a referral to a *Youth Partnerships* Agency Support Team. The support team is brought together to discuss ways of helping Spencer and to account for their previous (individual) interactions with Spencer.

This will involve the collection and handling of personal information. While it is not specified in the scenario, it is possible that some of this information may be defined as sensitive or health information. It may also involve the collection and handling of personal information about his mother. The information will be used/disclosed to identify a more coordinated and targeted set of services for Spencer.

In terms of the application of the privacy principles, the following comments are made.

- The purpose of *Youth Partnerships* is to design and test new ways for the education, youth and family support, justice, homelessness and mental health sectors to work more collaboratively to support individual young people experiencing problems. It is based upon improved information sharing in order to provide more coordinated, youth-centred services. A clear account of the purposes of *Youth Partnerships* needs to inform the activities of each demonstration sites.
- Clear purpose statements and collection notices are required to help establish compliance with the requirements of the collection principle.
- While it is expected that the functions and activities of organisations represented at the *Youth Partnerships* Agency Support Team are consistent with the purpose of *Youth Partnerships*, these should be articulated for clarity and transparency.
- *Youth Partnerships* is a consent-based initiative; the scenario describes the use of a consent form. Any consent form used must capable of meeting all of the requirements of fully informed consent. Assessment of the form's validity is required.
- Use and disclosure of personal information for the purposes of the scenario is expected to be for the 'primary purpose' of collection and, therefore, permitted. No secondary use/disclosures are identified in the scenario. However, full assessment will be necessary to ensure that all uses and disclosures have been identified and that they comply with privacy requirements.
- Data quality and data security compliance measures are not described in the scenario. At a minimum, data quality and security requirements must be specified at the level of each demonstration site and participating organisations must agree to comply with these requirements.
- Openness requires the availability of a clearly articulated privacy policy. This responsibility arises at a whole-of-initiative level but may be delivered at the level of each demonstration site. At this point, it is not clear whether it is necessary, feasible and desirable for a single *Youth Partnerships* privacy policy to be developed and disseminated or, instead, each for demonstration site to take responsibility for articulating a *Youth Partnerships* privacy policy at the local level.

[28] The scenario was developed by Keith Peters, Project Officer, Grampians Region.

- Individual young people need to be informed that they may seek access to/correction of personal information held about them under the *Youth Partnerships* initiative. While there are legislative rights to seek access/correction under privacy and FOI legislation, it is considered important that individuals are given access to information about themselves wherever possible without exercising their legal right to seek access. No information is provided about access/correction in the scenario. Where/as possible, a consistent approach should be developed across *Youth Partnerships* and communicated to all participants.
- Unique identifiers will not be generated as a consequence of *Youth Partnerships,* although it is likely that some government-issued identifiers will be collected/handled by participants (e.g. Medicare numbers when a health service is provided). Individual demonstration sites will need to take account of the unique identifiers principle.
- Anonymity is not practicable at the level of providing tailored, individual youth services to a young person. However, prior to the point of service delivery, it is important to ensure that personal information is not collected if anonymous interactions can be supported.
- Transborder data flows are not envisaged under *Youth Partnerships* as it is a Victorian-based initiative involving Victorian organisations. However, based on funding arrangements, some personal information may be provided to Australian government agencies. This will require further assessment.
- Sensitive/health information requires consent as a precondition to collection. As *Youth Partnerships* is a consent-based initiative, it is expected that this requirement will be met as a matter of course (subject to any consent being fully informed).

These comments are high level at this point, as the scenario does not contain enough detail to undertake a complete analysis 'end-to-end' and from a 'whole-of-information-lifecycle' perspective. Prerequisites for a mapping exercise include a full account of the participants/actors involved as well as a complete list of the personal information collected and handled.

Function of a Privacy Foundation

One of the most striking elements of the case scenario is the series of final questions it documents. These illustrate a number of points made throughout the PIA report, including:

- The benefits of developing a comprehensive and holistic approach to privacy for *Youth Partnerships*, based upon a clear privacy foundation;
- The desirability of providing specific information about the meaning and impact of 'privacy' to all stakeholders;
- The need to ensure (proactively) that there is a shared understanding of privacy prior to commencement of *Youth Partnerships'* implementation activities across each demonstration site;
- The need to communicate a clear account of the *Youth Partnerships'* approach to privacy to all participants;
- The need to ensure that *Youth Partnerships* privacy arrangements are reviewed and signed off by all relevant governance bodies and that this is communicated to participants;

- The desirability of providing basic information to participants about privacy compliance, common privacy issues and the steps that have been taken to ensure that *Youth Partnerships* will support good privacy practice;
- The benefits of providing privacy training, both at the level of introducing privacy and in terms of explaining how *Youth Partnerships* has incorporated privacy into its planning and implementation processes; and
- The need to support the demonstration site project officers through the development and publication of a range of privacy strategies, tools, policies and procedures.