Policy

Privacy

Version number	**V1.1**
Approved by	Executive
Date approved on	28/02/2017
Effective date	27/09/2018
Last amendment date	27/09/2018 (incorporating OVIC)
Review due date	
Related documents	Privacy Complaint Handling Procedure Privacy Impact Assessment Template CCTV Policy Appearance Release Form *Surveillance Devices Act 1999* PROV Takedown Procedure *Privacy and Data Protection Act 2014*
Business owner	Coordinator: Internal Compliance
Superseded documents	None
Registry file number	2015/0335

Table of Contents

1 Introduction

1.1 Purpose

The purpose of this document is to provide guiding principles for the collection and use of personal information at PROV. This will ensure that staff handle personal information appropriately and PROV meets its privacy obligations for all processes and new information systems as required under the *Privacy and Data Protection Act 2014*.

1.2 Scope

This policy is applicable to all PROV staff including contractors, consultants, and volunteers. It is applicable to all information systems used within PROV and any business process required to enable PROV to carry out its normal day to day business functions. It also includes photography undertaken for formal and informal functions.

1.3 Background

The Commissioner for Privacy and Data Protection (CPDP) formally adopted a "Privacy by Design" policy in 2014 to support information privacy management for all Victorian Public Sector Agencies. The ten Information Privacy Principles (IPPs) contained in Schedule 1 of the *Privacy and Data Protection Act 2014* guide the handling of personal information and are the basis for Privacy by Design. The policy required all agencies to consider their privacy obligations before the creation of any new process and/or network infrastructure involving the collection of personal information. With specific regard to this document, IPP 5 (Openness) required organisations to document policies on their management of personal information and to make the document available to anyone who asks for it.

In 2017 the functions of the Freedom of Information Commissioner and the Commissioner for Privacy and Data Protection were merged to become the Office of Victorian Information Commissioner (OVIC).

1.4 Key Terms

Personal Information: "Personal information means information or an opinion (including information or an opinion forming part of a database), that is recorded in any form 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 2001 applies." [1]
Privacy Impact Assessment (PIA) (template): Identifies potential privacy risks or barriers and risk mitigation strategies.
Sensitive Information: The following is classified as sensitive information: 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, criminal record.
Unique Identifier: An identifier (usually a number) assigned by an organisation to an individual to uniquely identify that individual for the purposes of the operations of the organisation (i.e. tax file number, driver's license number).

[1] Privacy Impact Assessment Template – Commissioner for Privacy and Data Protection – Page 2

1.5 Legislation and supporting documentation

Privacy and Data Protection Act 2014
Public Records Act 1973
Privacy by Design (PbD) Policy – Commissioner for Privacy and Data Protection 2014
Privacy by Design : Effective Privacy Management in the Victorian public sector (Background Paper) Commissioner for Privacy and Data Protection (OVIC website 2018)
Privacy Impact Assessment template – Commissioner for Privacy and Data Protection 2014

1.6 Responsibilities

Role	Responsibilities
All staff including contractors, consultants, and volunteers	• Providing a verbal or written Collection Notice when collecting personal information • Being aware of their privacy responsibilities under this Policy and the Complaints Handling Procedure • Referring all privacy complaints to the PROV Privacy Officer • Ensuring reasons for another staff member's personal leave are not published • Ensuring personal information collected is only used for the primary purpose for which it was collected or for another purpose permitted under IPP 2 (Use and Disclosure) • Ensuring the option to remain anonymous is always given when asking for feedback • Not requesting name identification when collecting demographic data except if permission has been granted • Using the Bcc function in bulk emails to non-government recipients where appropriate • Storing personal information in registered files • Seeking express permission to use photographs prior to publication • Ensuring it is clear that the PROV Privacy Policy does not apply to a third party site • Completing a PIA in the planning stage (pre-procurement) for any new information system design & architecture • Completing a PIA in the planning stage of any new business process involving the collection of personal information • Reviewing any existing business process involving the collection of personal information
PROV Privacy Officer	• Handling all privacy complaints • Ensuring an authorised Complaints Handling Procedure is communicated to all staff and placed on PROVide and in the BCS under Strategic Management function and Procedures activity • Updating the PROV Privacy Statement on the PROV website • Ensuring the PROV Privacy Policy appears on the PROV website

1.7 Summary of the 10 Information Privacy Principles

Collection	An organisation can only collect person information if it is necessary to fulfil its functions.
Use and Disclosure	Personal information can only be used and disclosed for the primary purpose for which it was collected or for a secondary purpose that you would reasonably expect or in other limited circumstances.
Data Quality	Organisations must keep personal information accurate, complete and up to date.
Data Security	Personal information must be protected from misuse, loss, unauthorised access, modification or disclosure. An organisation must take reasonable steps to destroy or permanently de-identify your personal information when it is no longer needed.
Openness	Organisations must have clearly expressed policies on the way they manage personal information.
Access and Correction	People have a right to seek access to their own personal information and to make corrections if necessary.
Unique Identifiers	Unique identifiers, usually a number, can facilitate data matching. Use of unique identifiers is only allowed where an organisation can demonstrate that the assignment is necessary to carry out its functions efficiently.
Anonymity	Where lawful and feasible, a person should have the option of transacting with an organisation without identifying themselves.
Transborder Data Flows	If a person's personal information travels outside Victoria, their privacy protection should travel with it.
Sensitive Information	This includes a person's racial or ethnic origin, political opinions and membership of political associations, religious or philosophical beliefs, membership of professional or trade associations or trade unions, sexual preferences or practices, and criminal record. The law puts special restrictions on its collection.

1.8 Seven Foundational Principles of Privacy by Design

Proactive not reactive, preventative not remedial	Using proactive not reactive measures by anticipating and working to prevent invasive events occurring in the first place.
Privacy as the default setting	Ensuring personal information is automatically protected in any given ICT system business practice or process. No individual action is required to protect privacy as it is inbuilt into the system, by default.
Privacy embedded into design	Privacy is 'built in' to the design of any new system and not added on as an afterthought. Privacy then becomes an essential component of the core functionality of the system being delivered.
Full functionality: positive-sum, not zero sum	Accommodates all legitimate interests and objectives in a positive sum "win-win" manner and not through an outmoded zero-sum approach where unnecessary compromises or trade-offs are made. This avoids false dichotomies, such as 'privacy versus security', by demonstrating that it is possible to have both.

End-to-security – full life cycle protection	Once privacy is embedded into systems and practices before personal information is collected and stored, the information is able to extend securely throughout the entire lifecycle of the information involved. The appropriate security measures are essential to privacy from start to finish. This ensures that all personal information is kept securely across its lifecycle from collection through to destruction.
Visibility and transparency – keep it open	The assurance that information-based public sector practices and technologies operate according to stated promises and objectives and that these are subject to independent investigation and verification. All of the collection and handling steps along the way are visible and transparent, to users and providers alike.
Respect for user privacy – keep it user centric	Managers, architects and operators should keep the interests of the individual at the forefront by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options, keeping it user-centric.

2 Policy Statements

All PROV staff, including contractors, consultants, and volunteers, must adhere to the ten Information Privacy Principles and Seven Foundational Principles of Privacy by Design developed by the Office of the Commissioner for Privacy and Data Protection and endorsed by the Office of the Victorian Information Commissioner.

The statements in this policy refer to processes used and records created by PROV as a State Government agency. Privacy requirements for records contained within the State Archive are covered by Section 9 of the *Public Records Act 1973*.

2.1 Collection Notices

A verbal and/or written Collection Notice must be provided when collecting personal information from an individual. The notice should be tailored to the circumstance and include:

- the purposes for which the information is collected
- to whom PROV usually discloses information of that kind
- any law that requires the particular information to be collected
- the main consequences (if any) for the individual if all or part of the information is not provided
- how the individual can gain access to their information
- PROV's contact details

2.1.1 **Example Collection Notice**

"Your personal information is being collected for the purposes of registering and administering a conflict of interest. It will be not used for any other purpose and will be managed in accordance with the *Privacy and Data Protection Act 2014* and PROV's Privacy Policy available at www.prov.vic.gov.au. You can seek access to this information by contacting the Privacy Officer."

2.2 Privacy Complaints

All PROV staff, including contractors, consultants, and volunteers, must:

- refer all privacy complaints immediately to the PROV Privacy Officer

2.3 Privacy Officer

The **PROV Privacy Officer** must:

- handle all privacy complaints
- ensure the PROV Takedown Procedure is completed for a complaint concerning the website or social media
- ensure an authorised Privacy Complaints Handling Procedure is communicated to all staff and placed on PROVide and in the BCS under the Strategic Management function and Procedures activity

2.4 Website

The **PROV Privacy Officer** must ensure that:

- the PROV Privacy Policy is up to date and is published on the PROV public website

- a Privacy Statement appears on the PROV website at all times and clearly shows the following for our own agency records and processes:
    - the purposes for which the information is collected
    - to whom PROV usually discloses information of that kind
    - any law that requires the particular information to be collected
    - the main consequences (if any) for the individual if all or part of the information is not provided
    - how the individual can gain access to their information
    - PROV's contact details

2.5 Closed Circuit Television surveillance (CCTV)

PROV seeks to protect people and assets in and around PROV property in the most effective manner possible including, where necessary, through the appropriate application of closed circuit television (CCTV) surveillance systems.

The primary security use of CCTV is to discourage and/or detect unlawful behaviour in and around PROV property thereby enhancing the safety and security of all people and property.

PROV's CCTV Policy provides detail on PROV's use of CCTV.

2.6 Internal Privacy

All PROV staff, including contractors, consultants, and volunteers, must:

2.6.1 **Leave Notifications**

Ensure reasons for another staff member's personal leave are not published (unless permission has been given).

2.6.1.1 Example

Jill Jolly rings her boss and advises she will not be in the office due to a migraine. If an email notification is required, (whether to other team members or to all staff) simply advise "Jill will not be in the office today".

2.6.2 **Photographs – New & Historical**

For any photograph that is intended to by published electronically, or in hard copy, permission must be sought from each staff member being photographed prior to publication using a *PROV Appearance Release Form. The Release Form applies to any event where images may be published externally. If permission has not been granted from everyone identifiable in the image, the photo cannot be used. Forms must be filed in Promotion & Outreach /*Photographs*/ Appearance Release Forms. No release form is required for internal staff events such as celebrations and meetings where there is no intention to publish. However, note that while consent is often implied, care must be taken to ensure that staff not wishing to be photographed are able to opt-out.

*found in Promotion & Outreach/Procedures/Appearance Release Form

2.6.2.1 **1.1.1.1 Example**

Jimmy Johnson is leaving after 25 years of service. His manager has put together a presentation of photos from all his time at PROV. His manager should check with Jimmy, and anyone who appears in the photos, to ensure they are comfortable with them appearing in the presentation. In this example, no release forms are necessary as the photographs will not be published.

2.7 Customer/Client Privacy

All PROV staff, including contractors, consultants, and volunteers, must:

2.7.1 Use and Disclosure

Ensure personal information collected is only used and disclosed for the primary purpose for which it was collected, or for purposes related to that primary purpose which are within reasonable expectations of persons who have provided the information, or for another purpose permitted under IPP 2 (Use and Disclosure) e.g. for law enforcement purposes or where required or authorised by another law. Keeping personal information for the purpose of recordkeeping is lawful.

2.7.2 Feedback & Surveys

Ensure the option to remain anonymous is always given when asking for customer/client feedback. Name identification must not be sought for questions regarding demographic data (i.e. cultural background, disability etc.).

2.7.3 Group Emails

Ensure care it taken when sending out bulk emails to non-government recipients. If you believe privacy will be breached use the BCC option.

2.7.3.1 Example

A group email is sent to members of the general public that have registered interest in attending a seminar. There is no need for anyone in the group to know each other's email address therefore the BCC option should be used.

2.7.4 Registration and Security

Ensure collected personal information (i.e. details on grant applications, mailing address lists, etc.) is stored in registered hard copy files. These files must be put away securely when not in use.

2.7.5 Events

Ensure that a Collection Notice is stated and displayed at any PROV event where photography or filming will occur.

Where photography or filming will occur at an event and may be used in the future for promotional purposes the organiser of the event must:

- Add a collection notice to the invitation
- Display a collection notice at the event itself
- Ensure that a signed consent form is obtained from individuals where the photographs are 'close-up' and are not a general crowd/audience photograph. In particular, a consent form must be obtained from the parents/guardians of children under the age of 18. Consent forms must clearly describe the possible uses of the photograph e.g. hard copy and/or online publication.

2.7.5.1 Sample Collection Notice

An example is:

FOR VISITORS AND GUESTS Events at the Victorian Archives Centre are photographed and recorded. Photos and recordings will be kept by Public Record Office Victoria and may be used for non-commercial promotional purposes including websites, publications and social media. Please inform the photographer if you do not want your photograph taken or your image recorded on film.

2.7.6 Third Parties

Ensure it is made clear that the PROV Privacy policy does not apply when using a third party site to collect information (i.e. event booking applications etc.).

2.8 New Process or Information System

All PROV staff, including contractors, consultants, and volunteers, must:

2.8.1 New Information System Design & Architecture

Complete a Privacy Impact Assessment (PIA) in the planning stage (pre-procurement) for any new information system design and architecture. Upon completion of the PIA, any technical specifications required for procurement must detail the specific privacy requirements for adherence to the *Privacy and Data Protection Act's* Information Privacy Principles and Privacy by Design principles.

2.8.2 New Process Involving the Collection of Personal Information

Complete a PIA in the planning stage of any new business process to ensure the principles of privacy are embedded into the process.

2.8.3 Existing Process Involving the Collection of Personal Information

Complete a review of any existing process involving the collection of personal information to ensure the IPPs are being adhered to. If breaches in processes are found, mitigation strategies must be determined and implemented immediately.

2.8.3.1 Privacy Impact Assessment (PIA)

The PIA for any new information system or business process must identify all personal information elements involved in the system and or process. The PIA must contain answers for the following questions:

- Is all the information collected necessary for the system/process?
- Is it lawful or practicable for the individual to remain anonymous for the purpose of the system/process?
- Will this program assign or collect a unique identifier?
- Is it necessary to assign a unique identifier to enable PROV to carry out the process?

End of Document