1.29 Information Privacy

Version 9.0

1. Purpose

This document outlines VICSES' obligations pertaining to the collection, management and disclosure of personal information.

2. Relevant to

All VICSES members

All contractors

3. Principle

VICSES is committed to the protection of the privacy of personal information. It will manage personal information in accordance with privacy laws.

4. Definitions

Freedom of Information: The *Freedom of Information Act 1982* (Vic), 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 its' agencies.

Information Privacy Principles: The Information Privacy Principles set out in Schedule 1 of the *Privacy and Data Protection Act 2014* (Vic). They outline how VICSES and other Victorian government agencies should collect, manage and disclose personal information. There are 10 Information Privacy Principles. See Guideline - *1.29-1 - Information Privacy Principles* for more information.

Personal Information: means information or an opinion, whether true or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion. Personal information can be almost any information linked to an individual, including name, address, sex, age, financial details, marital status, education or employment history.

Sensitive Information: a subset of personal information. Sensitive information means information or an opinion that relates to things like an individual's racial or ethnic origin, political opinions, religious beliefs, membership of a professional association or trade union, sexual preferences or criminal record.

5. References and Related Policies

Privacy and Data Protection Act 2014 (Vic)

Health Records Act 2001 (Vic)

Freedom of Information Act 1982 (Vic)

Surveillance Devices Act 1999 (Vic)

Privacy Act 1988 (Cth)

Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth)

Office of the Victorian Information Commissioner's Guidelines to the Information Privacy Principles

Victorian Public Sector Code of Conduct

Policy - 1.11 - Culture & Conduct

Procedure – 1.11-1 – Misconduct & Grievance

Policy – 3.23 – Records Management

6. Responsibilities

Role	Responsibility
VICSES Board Member	Responsible for ensuring VICSES has the appropriate support to maintain compliance with relevant privacy legislation.
Auditors - External	Authorised agencies only can request privacy audits in accordance with compliance to legislative and statutory scope of their work.
Auditors Internal	Authorised by VICSES management, Risk Audit Committee or Board, as required to conduct privacy audits.
VICSES Risk Audit Committee Member	Provides direction regarding the state of activities and compliance with VICSES information privacy policy.
Executive/Information Security & Governance Committee Member	• Responsible for ensuring the organisation's privacy posture is continuously improved. • Responsible for overseeing and approving privacy-related initiatives including compliance and audit activities. • Responsible for reporting on the status of privacy compliance, and related activities as appropriate to all stakeholders.
Chief Executive Officer	Accountable for ensuring VICSES staff and volunteers act in accordance with this policy* and applicable privacy legislation.
Manager Information Security & Governance	Responsible for maintaining this policy*, adherence of the organisation to relevant privacy legislation, promoting privacy law awareness throughout the organisation and accountable for handling and processing of privacy issues and complaints.
Freedom Of Information & Privacy Officer	Responsible for handling and processing privacy issues and complaints, as well as promoting privacy law awareness throughout the organisation. Assists in maintaining this policy* and to achieve adherence of the organisation to relevant privacy legislation.
Senior Managers	Responsible for ensuring they and their direct reports conduct their work in accordance with this policy* and relevant privacy legislation.

All members (including contractors and consultants)	Responsible for ensuring they observe and abide by the Information Privacy Principles set out in Schedule 1 of the Privacy and Data Protection Act 2014 (Vic). These Principles are outlined in the accompanying Guideline - 1.29-1 - Information Privacy Principles.
Third party goods and services suppliers.	Perform their work in accordance with this policy*.

* *Policy* refers to the Information Privacy Policy and its associated Standards and Procedures.

7. Policy

As a public agency, VICSES must collect, manage and disclose personal information as part of its everyday operations. This is to be expected and not discouraged. VICSES must ensure, however, that the personal information it collects is managed in a way that ensures the ongoing privacy of the individuals concerned.

To this end, VICSES will only collect, manage and disclose personal information in accordance with the requirements of the *Privacy and Data Protection Act 2014* (Vic) and the *Health Records Act 2001* (Vic) and, specifically, the Information Privacy Principles.

VICSES will endeavour to proactively embed privacy considerations into the design or implementation of new or amended systems and processes through the use of Privacy Impact Assessments.

Privacy breaches will be reported in accordance with *Procedure – 1.29-4 – Privacy Breach Notification* in order to mitigate their effects and prevent future occurrences.

Any complaints of a perceived breach of privacy in the workplace will be investigated by VICSES in accordance with *Policy - 1.11 - Culture & Conduct* and its associated *Procedure – 1.11-1 – Misconduct & Grievance* but will, ultimately, be judged against the requirements of the Information Privacy Principles and any other applicable legislation.

Privacy and Consent

Assessing whether the necessary consent has been given will depend on the circumstances of each case, but is generally defined by legislation.

The five elements of consent are: the individual has the capacity to consent and that the consent is voluntary, informed, specific and current. Under Section 3 of the Privacy and Data Protection Act, consent can be ‘expressed’ or ‘implied’.

Consent is not the only basis by which information can be collected or used. The Privacy and Data Protection Act allows the collection, use and disclosure of personal information in circumstances where consent has not, or cannot, be obtained. Examples include:

- when an organisation collects information necessary for its functions (IPP 1);
- when information is used for the primary purpose for which it was collected (IPP 2.1);
- when information is disclosed for one of the reasons outlined under IPP 2.1(a), (c)-(h); and
- when information is publicly available.

Recordings and Consent

Conversations are sometimes recorded, for example during online meetings, and the issue of consent becomes important.

Victoria follows the one-party consent rule, allowing individuals to record private conversations as long as one party to the conversation consents.

Section 6(1) of the Surveillance Devices Act 1999 states that if a person is not a party to a private conversation, that person is prohibited from secretly recording or using a device to listen to that conversation.

If a person who is a party to a private conversation records the conversation, it is not in breach of the surveillance legislation, however the publication or communication of any recording of a private conversation is prohibited.

8. Attachments

Guideline - 1.29-1 - Information Privacy Principles

Guideline - 1.29-2 - FOI and Privacy

Guideline - 1.29-3 - Use of Recording Devices

Procedure – 1.29-4 – Privacy Breach Notification

Form – 1.29-5 – Privacy Breach Notification

Procedure – 1.29-11 – Managing Misdirected Emails

Guideline – 1.29-12 – Preventing Misdirected Emails

9. Audit Requirements

Nil.

Effective Date: 15 August 2018	**Authorised by: Information Security & Governance Committee**
Review Date: 4 February 2028	**Owner: Manager Information Security & Governance**