​​

​​

Privacy Policy

Purpose

To provide a transparent framework for the collection, use and disclosure of personal information by Chameleon and it’s authorised representatives;

• To promote awareness of responsible personal information handling practices at Chameleon;

• To promote the responsible and transparent handling of personal information at Chameleon;

• To promote responsible data security practices at Chameleon.

Scope

This policy applies to all operations of Chameleon. It applies to the collection, use and disclosure of all personal information or data by Chameleon personnel including employees and independent contractors. Personal Information may be disclosed to third parties on a confidential basis where the disclosure is reasonably necessary so that that service provider may provide those services.

This policy does not apply to personal information or data which relate to the judicial or quasi-judicial functions of a court, tribunal, a Royal Commission, Board of Enquiry, has been made public or is legitimately already within the public domain or is a document of Chameleon under the meaning of the Freedom of Information Act 1982 (Vic).

# Policy Statement

Chameleon is committed to respecting the privacy of the personal information it collects in order to carry out its purposes, functions and activities. This policy sets out Chameleon’s commitment to compliance as well as details of how that commitment is to be carried out.

# Meaning of 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 and whether true or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

All personal and health information collected, used, held, disclosed or shared by Chameleon will be in accordance with the following Acts:

Privacy and Data Protection Act 2014 (Vic) and the

Privacy Act 1988

Specific disclosures will be made with consent or otherwise in accordance with the use and disclosure standards of the Privacy and Data Protection Act 2014, the Health Records Act 2001 and the Freedom of Information Act 1982.

## Chameleon will:

Only collect personal information that is necessary for Chameleon to carry out its functions and activities

• Use or disclose Personal Information as for the primary purpose of providing educational services, where the purpose is related or ancillary to the primary purpose, where consent is provided or where it may be permitted under the Act or the Privacy Act 1988 or required by the relevant legislation, and

Take reasonable steps to:

• Protect the personal information held from misuse, loss and from unauthorised access, modification

or disclosure, and

• Make sure that the personal information collected, used and disclosed is accurate, complete and up-to-date

• Maintain responsible data security practices at Chameleon.

• Ensure all personal information collected, held or shared by Chameleon must be done so in

accordance with this policy.

• Ensure the security of Personal Information and its proper storage, archiving or disposal in

accordance with appropriate recordkeeping standards and information technology safeguards.

• Be open and transparent about the Privacy and Data Protection Policy, about the type of personal

information Chameleon holds and what is done with such information.

• Enable individuals to access their data and make appropriate corrections, in accordance with

relevant access procedures.

# Privacy compliance training

All staff must complete or attend privacy training upon commencement of employment at or upon

provision to existing staff (whichever applies), and complete regular refresher training as directed.

# Workplace Procedures

The 10 Information Privacy Principles (IPPs) are the core of privacy law in Victoria and set out the minimum standard for how Victorian public sector bodies should manage personal information.

Short guide as stated by:

Short guide to the Information Privacy Principles

Guidance for individuals and the Victorian public sector

## Principle 1 – Collection

An organisation can only collect personal information if it is necessary to fulfil one or more of its functions. It must collect information only by lawful and fair means, and not in an unreasonably intrusive way. It must provide notice of the collection, outlining matters such as the purpose of collection and how individuals can access the information. This is usually done by providing a Collection Notice, which should be consistent with an organisation's Privacy Policy.

## Principle 2 – 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 would be reasonably expected. It can also be used and disclosed in other limited circumstances, such as with the individual's consent, for a law enforcement purpose, or to protect the safety of an individual or the public.

## Principle 3 – Data Quality

Organisations must keep personal information accurate, complete and up to date. The accuracy of personal information should be verified at the time of collection, and periodically checked as long as it is used and disclosed by the organisation.

## Principle 4 – Data Security

Organisations need to protect the personal information they hold from misuse, loss, unauthorised access, modification or disclosure. An organisation must take reasonable steps to destroy or permanently de-identify personal information when it is no longer needed.

## Principle 5 – Openness

Organisations must have clearly expressed policies on the way they manage personal information. Individuals can ask to view an organisation's Privacy Policy.

## Principle 6 – Access and Correction

Individuals have the right to seek access to their own personal information and to make corrections to it if necessary. An organisation may only refuse in limited circumstances that are detailed in the PDP Act. The right to access and correction under IPP 6 will apply to organisations that are not covered by the Freedom of Information Act 1982.

## Principle 7 – Unique Identifiers

A unique identifier is an identifier (usually a number) that is used for the purpose of identifying an individual. Use of unique identifiers is only allowed where an organisation can demonstrate that the assignment is necessary to

carry out its functions efficiently. There are also restrictions on how organisations can adopt unique identifiers assigned to individuals by other organisations.

## Principle 8 – Anonymity

Where lawful and practicable, individuals should have the option of transacting with an organisation without identifying themselves.

## Principle 9 – Transborder Data Flows

If an individual's personal information travels outside Victoria, the privacy protection should travel with it. Organisations can only transfer personal information outside Victoria in certain circumstances, for example, if the individual consents, or if the recipient of the personal information is subject to a law or binding scheme that is substantially similar to the Victorian IPPs.

## Principle 10 – Sensitive Information

The PDP Act places special restrictions on the collection of sensitive information. This includes racial or ethnic origin, political opinions or membership of political associations, religious or philosophical beliefs, membership of professional or trade associations or trade unions, sexual preferences or practices, and criminal record.

Organisations can only collect sensitive information under certain circumstances.