

|  |
| --- |
| Social Services Regulator and Interim Privacy Policy  |
| Meeting legislative privacy obligationsJuly 2024 |
|  |

Contents

[Overview 1](#_Toc169625346)

[To what and whom does this policy apply? 2](#_Toc169625347)

[What does the Regulator do? 2](#_Toc169625348)

[Definitions of personal, health and sensitive information 2](#_Toc169625349)

[Collection of personal and health information 3](#_Toc169625350)

[What the Regulator does with the information collected 5](#_Toc169625351)

[How the Regulator stores and protects information 5](#_Toc169625352)

[Access to and correction of information 6](#_Toc169625353)

[Making a complaint about a privacy incident (breach) 6](#_Toc169625354)

[How does the Regulator protect information transferred outside of Victoria? 6](#_Toc169625355)

[Workplace participant responsibilities 7](#_Toc169625356)

# Overview

The Social Services Regulator (**the Regulator**) collects, uses and discloses personal information (which includes sensitive information) and health information about the people using social services that it regulates and staff who work at these social services.

The Regulator acknowledges the sensitivity of information provided to it and is committed to protecting the privacy of this information in accordance with the law.

The Regulator is bound by privacy and other laws, including:

* *Social Service Regulations Act 2021*
* *Social Services Regulations 2023*
* *Social Services Regulation Transitional Regulations 2023*
* *Social Services (Supported Residential Services) Regulations 2024*
* *Privacy and Data Protection Act 2014*
* *Health Records Act 2001*
* *Children, Youth and Families Act 2005*
* *Charter of Human Rights and Responsibilities Act 2006*
* *Freedom of Information Act 1982.*
* *Victorian Data Sharing Act 2017*
* *Public Records Act 1973*

# To what and whom does this policy apply?

This policy applies to all personal (which includes sensitive) and health information collected, stored, used and disclosed by the Regulator while performing its functions under the *Social Services Regulation Act 2021*. This may include about any individual who interacts with social service providers, other government agencies and the Regulator.

This policy also applies to all personal and health information collected, stored, used and disclosed about people working for the Regulator. This includes the Regulator’s staff, secondees, labour hire, personnel, contractors, sub‑contractors and those on work experience and volunteers. These individuals are collectively referred to throughout this document as workplace participants.

# What does the Regulator do?

The Regulator is an independent statutory authority responsible for regulating social services in Victoria. The Regulator’s objects are to:

1. Promote and support the delivery of safe and effective social services in Victoria.
2. Monitor and enforce compliance with the requirements under the *Social Services Regulation Act 2021* and *Social Services Regulations 2023* which relate to the safe delivery of social services.
3. Protect the rights of people who use social services.
4. Minimize risks of avoidable harm caused by abuse or neglect in connection with the delivery of social services.
5. Encourage a culture of continuous quality improvement in the provision of social services.
6. Provide confidence to service users and the community in the safety and quality of social services.

The types of social services that the Regulator has oversight of includes disability services, community-based child and family services, child protection, homelessness services, family violence services, sexual assault services, out of home care services, and supported residential services.

The Regulator collects, uses, stores and discloses a range of personal and health information for the purposes of carrying out its statutory functions, which include:

1. Monitoring and enforcing compliance with the Social Services Standards.
2. Registering providers of social services.
3. Publishing information about registered social service providers on, and maintain, the Register.
4. Administering the worker and carer exclusion scheme (including the database of excluded workers and carers), based on a procedurally fair process for investigating and determining whether workers pose unjustifiable risks of harm to service users.
5. Collecting and analysing information about whether the Regulator’s objects are being achieved.
6. Sharing information for the purposes of effectively utilising regulatory intelligence, coordinating government responses in relation to social services, and reducing regulatory burden (where appropriate).
7. Other functions conferred on the Regulator under the *Social Services Regulation Act 2021* or any other Act.

# Definitions of personal, health and sensitive information

We are committed to protecting the privacy of your information and we are bound by Victorian laws, as well as other laws that impose specific obligations in regard to handling information. In Victoria, the *Privacy and Data Protection Act 2014* (Vic) and the *Health Records Act 2001* (Vic) are the primary legislation that regulates the information handling of personal and health information. The Regulator will manage your information in accordance with the Information Privacy Principles and Health Privacy Principles that provide standards for information collection, storage, access, transmission, disclosure, use and disposal as prescribed within these Acts.

### Personal information

Personal information is defined in the Privacy and Data Protection Act as 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 Actapplies.

### Sensitive information

Sensitive information is a subset of personal information. It is defined in the Privacy and Data Protection Act. It means information or an opinion 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, orientation or practices
* criminal record

that is also personal information.

### Health information

Health information is defined in the Health Records Act. Where information is health information and so is not caught by the Privacy and Data Protection Act, then the law is different in some respects. The Health Records Act defines health information as:

* information or an opinion about:
	+ the physical, mental or psychological health (at any time) of an individual; or
	+ a disability (at any time) of an individual; or
	+ an individual's expressed wishes about the future provision of health services to him or her; or
	+ a health service provided, or to be provided, to an individual

that is also personal information (see definition of personal information under the *Health Records Act 2001* below); or

* other personal information collected to provide, or in providing, a health service; or
* 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
* 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.
* the definition 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 generally or for the purposes of specified provisions of that Act.

Personal information is defined in the Health Records Act as information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion, but does not include information about an individual who has been dead for more than 30 years.

# Collection of personal and health information

The Regulator collects personal and health information as necessary for the purposes of carrying out its objects, functions and powers outlined under the *Social Services Regulation Act 2021* (under sections 7, 13 and 14).

The Regulator collects personal and health information only by lawful and fair means and not in an unreasonably intrusive way. If it is reasonable and practicable to do so, the Regulator collects personal and health information about an individual only from that individual.

When collecting information directly from an individual and when collecting information from someone else about an individual, the Regulator will take reasonable steps to ensure the individual is aware of why the information is being collected (including the purposes for the collection and any relevant laws requiring the collection), who it may be disclosed to, the main consequences if the individual does not disclose the information (if collecting information directly from the individual), and how the individual may contact the Regulator and gain access to the information collected. There may be exceptions in the Information Privacy Principles and the Health Privacy Principles in certain circumstances that do not require reasonable steps to be taken but this needs to be assessed on a case-by-case basis.

The Regulator typically collects information in the following ways:

* directly from the individual to which the information relates.
* where it is not reasonable or practicable to collect the information directly from the individual, information may be collected from a third party, such as the individual's authorised representative or a service provider.
* from social service providers, in the context of their notifications made to the Regulator to meet reporting requirements under the *Social Services Regulation Act 2021.*
* where information may be provided by a third party, such as individuals, other regulators or government agencies as permitted under the *Social Services Regulation Act 2021.*

The Regulator collects personal and health information for the purposes of carrying out its functions and meeting its statutory requirements. Unless the use or disclosure of personal or health information is for the primary purpose of collection, or it is for secondary purpose and one of the permissible exceptions under Information Privacy Principle 2.1 or Health Privacy Principle 2.2 applies, the Regulator removes identifying details from the information it collects.

### Collection of sensitive information

The Regulator may collect sensitive information where:

* the individual has consented to the collection;
* the collection is required or authorised under law (such as under the Acts listed on page 1);
* the collection is necessary to prevent or lessen a serious threat to the life or health of any individual, where the individual whom the information concerns is physically or legally incapable of giving consent to the collection or physically cannot communicate consent to the collection; or
* the collection is necessary for the establishment, exercise or defence of a legal or equitable claim.

The Regulator may also collect sensitive information about an individual if:

* the collection is necessary for research or the compilation or analysis of statistics relevant to government funded targeted welfare or educational services; or
* the information being collected relates to an individual's racial or ethnic origin and the purpose of the collection is to provide government funded targeted welfare or educational services; and
* there is no reasonably practicable alternative to collecting the information for either purpose; and
* it is impracticable for the organisation to seek the individual's consent to the collection.

### Types of information collected by the Regulator

The types of personal or health information the Regulator collects depends on the nature of the contact with the Regulator, services provided (where applicable) and statutory requirements of the department.

Personal information collected by the Regulator may include (but is not limited to):

* name, address and contact details;
* personal circumstances (age, gender and information about children);
* financial matters (payment and bank account details);
* identity (date and country of birth); and
* government identifiers.

The Regulator also collects health information if it is necessary to carry out its objects, functions and powers outlined under the *Social Services Regulation Act 2021* (sections 7,13, and 14).

# What the Regulator does with the information collected

The Regulator uses and discloses personal (including sensitive information) and health information for:

* the primary purpose for which it was collected; or
* a purpose related to that for which it was collected (secondary purpose) where the legislative requirements for using or disclosing for a secondary purpose are met.

The Regulator may use or disclose personal (including sensitive information) or health information when:

* the secondary purpose relates to the primary purpose of collection (or directly relates to the primary purpose in the case of sensitive or heath information) and an individual would reasonably expect the Regulator to use or disclose it in this way;
* the individual to whom the information is about has given consent for the use or disclosure; and/or
* the Regulator is required, authorised or permitted by or under law to use or disclose the information.

The information collected might be able to be shared within the Regulator between different business units if business units comply with the Information Privacy Principles or Health Privacy Principles before doing so. Such information may also be shared from the Regulator to service providers to enable efficient and effective delivery of quality services in compliance with the Information Privacy Principles and Health Privacy Principles.

The Regulator collects, uses, holds and discloses personal and health information about a range of matters, including, but not limited to:

* individuals who use the social services it regulates;
* managing compliance investigations;
* managing audits;
* employment and personnel matters concerning the Regulator’s staff and contractors;
* correspondence from members of the public to the Regulator, Ministers and Parliamentary Secretaries;
* complaints made and the feedback provided;
* requests made under the *Freedom of Information Act 1982;*
* investigating incidents for example, those that occur during the delivery of social services;
* meeting its legislative requirements;
* policy development and research; or
* meeting the reporting requirements of government and external oversight agencies.

There are circumstances where the Regulator is authorised and/or required by law to collect, use, hold or disclose an individual’s information.

Wherever it is lawful and practicable, an individual must be given the option of remaining anonymous when interacting with the Regulator. A circumstance where it is not practicable for the individual to remain anonymous is where the Regulator is responsible for providing a full range of specific and coordinated services to the individual.

# How the Regulator stores and protects information

The Regulator has security measures designed to protect personal and health information from misuse, loss, unauthorised access, modification or disclosure. The Regulator must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose in line with *the Public Records Act 1974*. In relation to health information, the Regulator must take reasonable steps to destroy or permanently de-identify health information if it is no longer needed for the purpose for which it was collected or any other purpose authorised by the Health Records Act, the regulations made under the Health Records Act, or any other law.

The regulator takes reasonable steps to ensure that any personal and health information it collects, uses and discloses is accurate, complete and up to date, and having regard to the purpose for which health information is to be used, that it is relevant to the Regulator’s functions.

# Access to and correction of information

An individual may ask for access to their information or request a correction to their information by contacting the Regulator through:

* the Regulator’s area that has the information (where known)
* emailing the Freedom of Information officer <enquiries@ssr.vic.gov.au>.

When contacted, the Regulator will let the individual know whether it holds information about the individual and any further steps that that individual should take to obtain access to the information.

If a query relates to an individual’s health information, this information will be held directly by the public health service provider. In this situation it would be more appropriate to make contact directly with the health service provider.

# Making a complaint about a privacy incident (breach)

An individual or organisation may make a complaint about a potential privacy incident (breach) by contacting the Regulator’s Legal Services by emailing <enquiries@ssr.vic.gov.au>.

Staff members of the Social Services Regulator can also lodge a complaint on via enquiries@ssr.vic.gov.au.

The team can also provide advice in relation to information sharing and privacy matters for the Regulator’s staff.

The Regulator undertakes to resolve privacy complaints and breaches in a timely and fair manner.

An individual may also make a privacy complaint to:

* the Health Complaints Commissioner in relation to a complaint relating to health information: 1300 582 113.
* the Office of the Victorian Information Commissioner in relation to a complaint relating to personal or sensitive information:1300 666 444.

# How does the Regulator protect information transferred outside of Victoria?

The Regulator adheres to the requirements of the Privacy and Data Protection Act and Health Records Act when transferring personal and health information outside of Victoria.

The only circumstances in which personal and health information may be transferred or stored outside of Victoria is when the transfer or storage meets one (or more) of the following criteria:

* the Regulator reasonably believes that the recipient of the information is subject to a law, binding scheme or binding contract that provides substantially similar protection to the Privacy and Data Protection Act or Health Records Act;
* the individual has provided consent to the transfer;
* the transfer is necessary for the performance of a contract between the individual and the Regulator, or for the implementation of pre-contractual measures taken in response to the individual's request;
* the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the Regulator and a third party;
* the transfer is for their benefit of the individual, and it is impracticable to obtain the individual’s consent to the transfer, but if it were practicable to obtain consent the individual would be likely to give it;
* the Regulator has taken reasonable steps to ensure that information which it has transferred will not be held, used or disclosed by recipients inconsistently with the Information Privacy Principles or Health Privacy Principles; and
* in the case of health information, the transfer is required or authorised by law.

# Workplace participant responsibilities

It is every workplace participant’s responsibility to familiarise themselves with the Information Privacy Principles set out in the Privacy and Data Protection Actand the Health Privacy Principles set out in the Health Records Actand to ensure that they comply with them. Online training is available on the Regulator’s intranet on the Privacy and Data Protection Act. Every staff member must also comply with this policy and contain and report any privacy incidents as soon as they become aware of them.