Every child, every opportunity

Privacy Policy

[Service] are bound by the [relevant legislation] as well as other laws that impose specific obligations in regard to handling personal and health information that directly or indirectly identifies a person. The privacy policy and principles in this document are in accordance with these laws.

[Service] is committed to protecting the privacy of personal and health information. This Privacy Policy embodies this commitment.

The policy supports the [Service's] need to collect information and the right of the individual to privacy. It ensures that the [Service] can collect personal and health information necessary for its services and functions, while recognising the right of individuals to have their information handled in ways that they would reasonably expect and in ways that protect the privacy of their personal and health information.

Policy

Personal and health information is collected and used by the [Service] for the following purposes:

- to provide services or to carry out [Service to input] functions
- to assist [Service] and it's employees to fulfil its duty of care to children
- to plan, fund, monitor and evaluate services and functions
- to comply with DEECD reporting requirements
- to investigate incidents in schools and/or defend any legal claims against the service, or its employees

[Service] has adopted the ten information privacy principals (IPP) developed by the Office of the Victorian Privacy Commissioner (**www.privacy.vic.gov.au** and search 'IPP') as minimum standards in relation to handling personal and health information. In broad terms, this means that [Service]:

- collect only information which is required for a specified primary purpose
- ensure that the person supplying the information knows why the information is collected and how it will be handled
- use and disclose it only for the primary or a directly related purpose, or for another purpose with the person's consent (unless otherwise required, permitted or authorised by law)
- store it securely, protecting it from unauthorised access retain it for the period authorised by the *Public Records Act 1973*, and take reasonable steps to permanently de-identify personal or health information when it is no longer needed
- provide people with access to their own personal information and permit people to seek corrections if necessary. This will usually be handled under the *Freedom of Information Act 1982*. For DEECD services not covered by this Act, access will be available as prescribed by the Victorian privacy laws.

[Service] in collecting personal and health information will:

- address the privacy issues relevant to their functions and only collect and use this information in accordance with the privacy principles
- manage this information according to privacy policies created for the area of service DEECD provides in accordance with the privacy principles.

[Service] in using personal and health information but do not directly collect personal and health information will apply the privacy principles when handling personal and health information.

Research: [Service] will usually only use or disclose an individual's personal or health information for research or the compilation of statistics with the individual's consent. When research or the compilation of statistics which is in the public interest cannot be undertaken with de-identified information, and where it is impractical to seek the individual's consent, the research or compilation of statistics will be carried out in accordance with the National Statement on Ethical Conduct in Research Involving Humans issued by the National Health and Medical Research Council (1999) and in accordance with the Health Services Commissioner guidelines.

Complaints

A complaint about information privacy is an expression of dissatisfaction with [Service] procedures, staff, agents or quality of service associated with the collection or handling of personal or health information. [Service] will be efficient and fair when investigating and responding to information privacy complaints. The process for investigation and response to these complaints is set out in [Service to input] .

Principles

The key Information Privacy Principles (IPPs) and Health Privacy Principles (HPPs) Principles are listed here. Only the key principles have been selected and are provided in summary. The full exceptions qualifying many of the principles are not included.

Collection: [Service] must collect only personal and health information that is necessary for performance or functions. Individuals should be told why this information is required, what it will be used for and that they can gain access to their personal and health information.

Use and disclosure: [Service] must only use or disclose personal and health information:

- for the primary purpose for which it was collected
- for a related secondary purpose (which must be a directly related purpose in the case of health or sensitive information) that the person would reasonably expect
- with the consent of the person
- unless otherwise required, permitted or authorised by law principles

Data quality: [Service] must make sure personal and health information is accurate, complete and up-to-date.

Data security: [Service] must take reasonable steps to protect personal and health information from misuse, loss, unauthorised access, modification and disclosure.

Openness: [Service] must document clearly expressed policies on management of personal and health information and make these policies available to anyone who asks for them.

Access and correction: Individuals have a right to seek access to their personal and health information and make corrections.

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 Medicare numbers are examples. Unique identifiers can facilitate data matching. Data matching can diminish privacy. Privacy laws limit the adoption and sharing of unique numbers. [Service] will limit the use of unique identifiers as required by the Victorian privacy laws.

Anonymity: When lawful and practicable, individuals should be able to remain anonymous in transactions with services.

Transborder data flows: Transfer of personal and health information outside Victoria is restricted by privacy laws. Personal and health information may be transferred only if the recipient protects privacy under standards similar to Victoria's IPPs/HPPs.

Sensitive information: *The Information Privacy Act 2000* restricts collection of sensitive information about an individual's racial or ethnic origin, political views, religious beliefs, sexual preferences, membership of groups or criminal record. [Service] will apply IPP10 when collecting and handling sensitive information.