Caulfield South Primary School

C.S.P.S.

Privacy Policy

Rationale:

The Department of Education and Training (the Department) is committed to protecting the personal and health information that we collect, hold, manage, use, disclose and transfer.

This policy supports the Department's need to collect information and the right of the individual to privacy.

It ensures that the Department 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 their personal and health information.

This policy supports staff to act in accordance with the Code of Conduct for Public Sector Employees which requires staff to demonstrate the value of respect by maintaining confidentiality and treating private information properly. Staff treat information properly by complying with legislation and policies relating to dealing with personal and health information.

Scope

This policy sets out how the Department is to collect, hold, manage, use, disclose or transfer personal and health information in accordance with the Information and Health Privacy Principles contained within the Privacy and Data Protection Act 2014 (Vic) and the Health Records Act 2001 (Vic)

The Department has also developed a schools' privacy policy which focuses upon information handling in schools; see the Schools' Privacy Policy.

Audience

All Departmental corporate staff must act in accordance with this policy.
Departmental school staff must act in accordance with the Schools' Privacy Policy.

Compliance

The Department must collect and handle personal information and health information in accordance with the Privacy and Data Protection Act 2014 (Vic) and the Health Records Act 2001 (Vic) unless otherwise required by law.

Accountable Officer

The Accountable Officer for this policy is the Executive Director, Integrity, Assurance and Executive Services Division (IAESD). The Accountable Officer is responsible for the:

- development of this policy
- implementation of any supporting protocols, processes and guidelines
- ongoing monitoring of compliance with this policy.

Review

This policy will be reviewed and updated from time to time to take account of new laws, technology and processes. The review process will be completed by the Privacy team within IAESD, with oversight provided by the Information Management Technology Committee (IMTC).

Contact

For more information about this policy, contact the Department's Privacy team on privacy@edumail.vic.gov.au.

Key definitions

Throughout this policy:

- **Health information** means information or opinion about a person's physical, mental or psychological health or disability that is also personal information. This includes information or opinion about a person's health status and medical history.
- **Personal information** means recorded information or opinion, whether true or not, about a person whose identity is apparent, or can reasonably be ascertained, from the information. The information or opinion can be recorded in any form.
- **Sensitive information** means information or an opinion that is also personal information about a person's racial or ethnic origin, political opinions, religious beliefs or affiliations, philosophical beliefs, sexual orientation or practices, membership of a political association, professional or trade association, or trade union, or an individual's criminal record.
- **Victorian privacy law** refers to the Privacy and Data Protection Act 2014 (Vic) and the Health Records Act 2001 (Vic) collectively. There are additional Acts which have privacy implications and are listed in this policy under the under Associated Legislation and Schemes.

- **Privacy impact assessment** means an assessment that identifies and assesses the privacy impacts of any system or software that handles personal, sensitive or health information.

Policy

Personal and health information is collected and used by the Department for the following purposes:

- to plan, fund, implement, monitor, regulate and evaluate the Department's services and functions
- to fulfil statutory and other legal obligations
- to comply with reporting requirements
- to investigate incidents in schools and/or defend any legal claims against the Department, its schools or its employees.

The Department has adopted the Information Privacy Principles (IPPs) and Health Privacy Principles (HPPs) in the Privacy and Data Protection Act 2014 (Vic) and the Health Records Act 2001 (Vic) respectively as minimum standards when dealing with personal and health information.

Adopting the IPPs and HPPs means that, subject to some exceptions (see Information and Health Privacy Principles), the Department must not commit an act, or engage in a practice, that contravenes an Information and/or Health Privacy Principle in respect of personal and/or health information collected, held, managed, used, disclosed or transferred by the Department unless otherwise permitted by law.

Information and health privacy principles

The Information and Health Privacy Principles most relevant to the Department are summarised as follows:

Collection of personal information

The Department will only collect personal information if the information is necessary for one of its functions or activities as set out in the Education and Training Reform Act 2006 (Vic), relevant Ministerial Orders and other applicable legislation.

Where the personal information of an individual is collected, reasonable steps should be taken to ensure that the individual is aware of:

- the identity of the Department and how to contact it
- the fact that the individual is able to gain access to the information
- who the Department usually discloses information of that kind to
- the purposes for which the information is being collected
- any law that requires the particular information to be collected

- the main consequence (if any) for the individual if all or part of the information is not provided to the Department.

Collection of health information

The Department will only collect health information if the information is necessary for one of its functions or activities and:

- the Department has gained consent from the individual; or
- collection is necessary to prevent or lessen a serious threat to the life, health, safety or welfare of any individual; or
- collection is necessary to prevent or lessen a serious threat to public health, safety or welfare; or
- collection is necessary for the establishment, exercise or defence of a legal or equitable claim.

Where the health information of an individual is collected, reasonable steps are taken to ensure that the individual is aware of:

- the identity of the Department and how to contact it
- the fact that the individual is able to gain access to the information
- the purposes for which the information is being collected
- who the Department usually discloses information of that kind to
- any law that requires the particular information to be collected
- the main consequence (if any) for the individual if all or part of the information is not provided to the Department.

Use and disclosure

The Department must only use or disclose personal and health information for the primary purpose for which it was collected, unless it falls within an exception, including where use and disclosure is:

- for a related secondary purpose and the individual would reasonably expect the Department to use or disclose the information for that secondary purpose; or
- with the consent of the individual; or
- necessary for research, or the compilation of statistics, in the public interest; or
- reasonably necessary to carry out a law enforcement function; or
- otherwise required, permitted or authorised by law. For example, the Department may be required to share information to:
- fulfil its duty of care to students, staff and visitors;
- provide a safe workplace in accordance with occupational health and safety law; or
- assess a risk of family violence or for a child wellbeing or safety purpose.

In cases where the use or disclosure is necessary for research or the compilation of statistics in the public interest, the Department will seek consent of each of the individuals involved. Where it is impracticable to seek the individual's consent and when the research or the compilation of statistics cannot be undertaken with de-identified information, the research or compilation of statistics will be carried out in accordance with the National Health Medical Research Council's National Statement on Ethical Conduct in Research Involving Humans, or for health information, in accordance with the Statutory Guidelines on Research.

Data quality

The Department values information as an important resource. Accordingly, the Department must take reasonable steps to ensure that the personal and/or health information it collects, uses or discloses is accurate, complete, up to date and relevant to the Department's functions or activities.

For example, it is the Department's practice to collect personal information from each individual concerned, rather than relying on other data sources, to ensure that names and other details are accurately recorded.

Data security

The Department is guided by the principle that all information is well governed and managed. Accordingly, the Department must take reasonable steps to protect the personal and/or health information it holds from misuse and loss, unauthorised access, modification or disclosure. The Department will destroy or permanently de-identify personal and/or health information if the Department no longer needs the information.

The Department requires that a Privacy Impact Assessment is conducted for all new and significantly changed processes that involve personal, sensitive or health information. It also requires that information assets recorded in the Department's Information Asset Register are assigned data classifications. Data classifications determine what level of security is required for each type of information.

Privacy incidents are confirmed or suspected actions of information handling that are inconsistent with the IPPs and/or HPPs. The Department's response to a privacy incident will focus on protecting personal and sensitive information and may require support by the information security team and other areas of the Department in order to resolve the incident. To report a suspected privacy incident, please email privacy@edumail.vic.gov.au.

Openness

To enable greater access to government decisions, the Department's information should be easy to find, access and use. This means that the Department must have, and make available, clearly expressed policies on its management of personal and health information.

On request, the Department must take reasonable steps to advise individuals, in general terms:

- what sort of personal information it holds about them
- for what purposes such information has been collected
- how it collects, holds, uses and discloses that information.

Access and correction

Individuals have a right to request access to, and to correct, their personal and health information held by the Department. Most requests to access and/or correct information held by the Department are processed in accordance with the Freedom of Information Act 1982 (Vic).

Parents, guardians and informal carers of students at Victorian government schools are, in most instances, entitled to school reports and other school communications ordinarily provided to a parent, unless a court order restricts this right. For more information, see Requests for information about students.

If a parent, guardian or informal carer wishes to request other types of documents held by Victorian Government Schools (for example staff diary notes, incident reports, counselling notes) the individual should be advised to make a Freedom of Information request.

In some cases, a student may be determined by a Principal (or nominee) to be a mature minor and able to make decisions independently about their own information. For more information, see Decision making by mature minors.

Unique identifiers

The Department limits its adoption and sharing of unique identifiers. The preferred unique identifier for the Department is the Victorian Student Number (VSN).

The Department will:

- not assign unique identifiers to individuals unless the assignment is necessary to enable it to carry out its functions efficiently or is otherwise required by law
- only adopt (as its own unique identifier of an individual), use or disclose a unique identifier assigned by another organisation in limited circumstances.

Anonymity

Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering into transactions with the Department, as long as this does not impede the Department's ability to carry out its functions.

As an example, people can request a policy or other non-sensitive document from the Department without having to provide their name, as long as they have supplied a means by which the Department can send them the document.

Transfer of information outside Victoria

The Department will only transfer personal and/or health information about an individual to someone who is outside Victoria in limited circumstances. Specifically, the Department should only transfer personal and/or health information outside Victoria if:

- the individual consents to the transfer;
- the Department reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which is very similar to the Victorian privacy law; or
- the Department has taken reasonable steps to ensure that the transferred information will not be held, used or disclosed inconsistently with the Victorian privacy law.

In cases where personal and/or health information is being transferred to a jurisdiction whose privacy requirements are inconsistent with Victorian privacy law, the Department requires that a Privacy Impact Assessment be undertaken before the data is sent.

Sensitive information

The Department will only collect sensitive information in limited circumstances. For example, the Department can collect sensitive information if the individual has consented or if the collection is required by law.

Charter of Human Rights and Responsibilities

When any decision is made in relation to personal, health or sensitive information, such as to use or disclose of that information, the decision-maker should give proper consideration to the Charter of Human Rights and Responsibilities Act 2006.

Some guidance on how to apply the Charter when making a decision is available through the Charter of Human Rights and responsibilities - Guidelines for Legislation and Policy Officers in Victoria and other Departmental guidance.

Associated legislation and schemes

Child Wellbeing and Safety Act 2005 (Vic) - Part 6A Information Sharing and Part 7A Child Link Register

In the first half of 2021, prescribed programs/services within the Department will become an information sharing entity (ISE) in accordance with the Child Wellbeing and Safety (Information Sharing) Amendment Regulations 2020 (Vic) which will enable ISEs to collect, use and disclose information with other ISEs for the purpose

of promoting the wellbeing or safety of a child/group of children, subject to meeting a legislative threshold.

The Child Information Sharing Scheme (CISS) broadens the circumstances in which information may be shared to support the wellbeing or safety of children. In doing so, the CISS aims to:

- improve early identification of issues/risks and enable earlier support for children and families
- promote a shared responsibility for children's wellbeing and safety across the service system
- increase collaboration and support integration between services involved with children and families
- support children's participation in services.

The Child Link Register is being developed along with the Child Information Sharing Scheme and will be operational for authorised Child Link users in the Department, schools and early childhood settings, from 2022.

The Child Link Register will improve child wellbeing and safety outcomes for children born or resident in Victoria by monitoring and supporting their participation in government-funded programs and services. The Child Link Register will allocate a unique identifier to each child, as there is no existing common unique identifier across government service systems that currently performs this function.

The Child Wellbeing and Safety (Information Sharing) Regulations are available from the Victorian Legislation website and the Child Information Sharing Scheme Ministerial Guidelines are also available online. Further information is also available online about the Child Information Sharing Scheme.

Family Violence Protection Act 2008 – Part 5A Information Sharing and Family Violence Information Sharing Guidelines

In the first half of 2021, prescribed programs/services within the Department will become an information sharing entity (ISE) in accordance with the Family Violence Protection (Information Sharing and Risk Management) Amendment Regulations 2020 (Vic) which will enable ISEs to collect, use and disclose information with other ISEs for the purpose of assessment or management of family violence and to hold perpetrators to account.

The Family Violence Information Sharing Scheme (FVISS) is designed to minimise the legislative barriers that had previously prevented the timely and effective sharing of information in cases of family violence or in circumstances where the risk of family violence is present. FVISS helps authorised organisations to assess and manage family violence risk.

A Multi-Agency Risk Assessment and Management Framework (MARAM) has been developed to help service practitioners to assess and manage family violence risk, including how to understand the appropriate application of the FVIS and CIS schemes in family violence situations. This framework applies to the Department in its entirety as a 'framework organisation'.

The Family Violence Protection Act and the Family Violence Protection (Information Sharing and Risk Management) Regulations 2018 are available from the Victorian Legislation website. Guidance on sharing information in the context of family violence can be found in the Child Information Sharing Scheme Ministerial Guidelines and further information is also available online about the Family Violence Information Sharing Scheme and MARAM.

The CISS, FVISS and MARAM are scheduled to commence in the first half of 2021 (at a date still to be determined), and will add to the existing suite of legislative permissions that enable confidential information to be shared. Targeted support and training for prescribed workforces, including relevant departmental program areas, will be provided by the Department in the lead up to commencement.

The Notifiable Data Breaches scheme

The Notifiable Data Breaches (NDB) scheme came into effect on the 22nd of February 2018 and requires entities captured by the scheme to notify the Office of the Australian Information Commissioner (OAIC) and affected individuals of any data breach which are likely to result in serious harm to individuals whose personal information is involved in the breach.

The NDB scheme applies to entities that have obligations to protect the personal information they hold under the Privacy Act 1988 (Cth). This includes Australian Privacy Principle (APP) entities, credit reporting bodies, credit providers and tax file number (TFN) recipients. As a Victorian government agency, the Department is subject to this scheme only in the case of breaches involving TFNs.

Further information is available at: Office of the Australian Information Commissioner.

General Data Protection Regulation (GDPR)

The European Union (EU) General Data Protection Regulation (GDPR) is designed to align data privacy laws across the EU and offer enhanced privacy protections for individuals in the EU. The GDPR came into effect on 25 May 2018.

The GDPR applies to the data processing activities of businesses, regardless of size, that are data processors or controllers with an establishment in the EU or that process or control the personal data of data subjects that reside in the EU regardless of the location of the business.

The GDPR makes entities accountable for their data processing activities, regardless of their location, when processing the personal data of individuals in the EU. This means that it can apply in the case of the Department handling information of EU or Australian citizens who are located within the EU; however it does not apply for EU citizens who are located in Australia.

If you have any further queries regarding the GDPR as it applies to the Department's activities please contact the Privacy Team. Further information is available at Office of the Victorian Information Commissioner, Office of the Australian Information Commissioner and EU GDPR.

Complaints

The Department will be efficient and fair when investigating and responding to information privacy complaints. The Department will investigate and respond to complaints in accordance with the Department's information privacy complaints handling process.

More information

For more information about this policy, contact the Department's Privacy team on privacy@edumail.vic.gov.au or (03) 8688 7967.

Schools' Privacy Policy

Privacy and Data Protection Act 2014 (Vic)

Health Records Act 2001 (Vic)

Office of the Victorian Information Commissioner

Office of the Health Complaints Commissioner

Evaluation

This policy will be reviewed again in 3 years.