updated

ST PATRICK'S PRIMARY SCHOOL

Privacy Policy

Policy Background

St Patrick's Primary School is bound by the Australian Privacy Principles contained in the **Privacy Act 1988 (Cth)** and as such may, from time to time, review and update this Privacy Policy to take account of new laws and technology, changes to schools' operations and practices and to ensure it remains appropriate to the changing school environment.

St Patrick Primary School's Policy

St Patrick's Primary School is committed to the Australian Privacy Principles and keeping personal and sensitive information confidential.

It is our policy that:
- all personal and sensitive information is handled in accordance with the Australian Privacy Principles;
- a Privacy Officer be appointed to deal with issues of privacy; and
- the School have appropriate systems and procedures in place to deal with any privacy issues, such as a breach.

Definitions

Act	the **Privacy Act 1988 (Cth)**
Australian Privacy Principles (APPs)	the 13 APPs set out in Schedule 1 of the Act.
Data breach	the loss, unauthorised access to, or disclosure of, personal information.
Loss	accidental or inadvertent loss of personal information likely to result in unauthorised access or disclosure. For example, an employee leaves a copy of a document or a device on public transport. If data can be deleted remotely or is encrypted it will not constitute an NDB.
Notifiable Data Breach (NDB)	a data breach that is likely to result in serious harm to any of the individuals to whom the personal information relates. A NDB occurs when personal information held by an organisation is lost or subjected to unauthorised access or disclosure. In such circumstances, the School must notify the Office of the Australian Information Commissioner (OAIC) and affected individuals as required under the **Privacy Amendment (Notifiable Data Breaches) Act 2017**.
OAIC	the **Office of the Australian Information Commissioner**.
Personal information	information or an opinion in any form about an identifiable individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not.
Sensitive information	information about 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 orientation or practices, or criminal record, or health information, genetic information or biometric information.
Serious harm	is determined with regard to the following list of relevant matters as provided for in section 26WG of the **Privacy Amendment (Notifiable Data Breaches) Act 2017**: • the kind or kinds of information; • the sensitivity of the information; • whether the information is protected by one or more security measures; • if the information is protected by one or more security measures—the likelihood that any of those security measures could be overcome; • the persons, or the kinds of persons, who have obtained, or who could obtain, the information; • if a security technology or methodology was used in relation to the information and was designed to make the information unintelligible or meaningless to persons who are not authorised to obtain the information; • the likelihood that the persons, or the kinds of persons, who: • have obtained, or who could obtain, the information; and • have, or are likely to have, the intention of causing harm to any of the individuals to whom the information relates; • have obtained, or could obtain, information or knowledge required to circumvent the security technology or methodology;

- the nature of the harm;
- any other relevant matters.

Unauthorised access — personal information accessed by someone who is not permitted to have access. This could include an employee of the entity, a contractor or external third party (such as hacking).

Unauthorised disclosure — where an entity releases/makes visible the information outside the entity in a way not permitted by the **Privacy Act**. For example, N employee accidently publishes a confidential data file containing personal information on the internet.

Provisions

The School will collect, hold, use and disclose personal information, as set out in this Privacy Policy.

What kinds of personal information does the School collect and how does the School collect it?

The type of information the School collects and holds includes (but is not limited to) personal information, including health and other sensitive information, about:

Students and parents and/or guardians (Parents) before, during and after the course of a student's enrolment at the School, including:
- name, contact details (including next of kin), date of birth, previous school and religion;
- medical information (e.g. details of disability and/or allergies, and details of any assistance the student receives in relation to those disabilities, absence notes, medical reports and names of doctors);
- conduct and complaint records, or other behaviour notes, school attendance and school reports;
- information about referrals to government welfare agencies;
- counselling reports;
- health fund details and Medicare number;
- any court orders;
- volunteering information;
- photos and videos at school events.

Job applicants, staff members, volunteers and contractors, including:
- name, contact details (including next of kin), date of birth and religion;
- information on job application;
- professional development history;
- salary and payment information, including superannuation details;
- medical information (e.g. details of disability and/or allergies, and medical certificates);
- complaint records and investigation reports;
- leave details;
- photos and videos at school events;
- workplace surveillance information; and
- work emails and private emails (when using work email address) and Internet browsing history.

Other people who come into contact with the School, including:
- name and contact details; and
- any other information necessary for the particular contact with the School.

Personal information you provide
The School will generally collect personal information held about an individual by way of forms filled out by Parents or students, face-to-face meetings and interviews, emails and telephone calls. On occasions people other than Parents and students (such as job applicants and contractors) provide personal information to the School.

Personal information provided by other people
In some circumstances, the School may be provided with personal information about an individual from a third party, for example, a report provided by a medical professional or a reference from another school. The type of information the School may collect from another school may include:
- Academic records and/or achievement levels
- Information that may be relevant to assisting the new school meet the needs of the student, including any adjustments.

Exception in relation to employee records
Under the **Privacy Act 1988 (Cth)**, the Australian Privacy Principles do not apply to an employee record. As a result, this Privacy Policy does not apply to the School's treatment of an employee record where the treatment is directly related to a current or former employment relationship between the School and an employee. The School handles staff health records in accordance with the Health Privacy Principles in the **Health Records Act 2001 (Vic)**.

Anonymity
The School needs to be able to identify individuals with whom it interacts and to collect identifiable information about them to facilitate the delivery of schooling to its students and its educational and support service, conduct the job application process and fulfil other obligations and processes. However, in some limited circumstances some activities and interactions with the School may be done anonymously where practicable, which may include making an inquiry, complaint or providing feedback.

How will the School use the personal information you provide?

The School will use personal information it collects from you for the primary purpose of collection, and for such other secondary purposes that are related to the primary purpose of collection and reasonably expected, or for which you have consented.

Students and Parents
In relation to personal information of students and Parents, the School's primary purpose of collection is to enable the school to provide a quality Catholic education to the student, exercise its duty of care and perform necessary associated administrative activities, which will enable students to take part in all the activities of the School. This includes satisfying the needs of Parents, the needs of the student and the needs of the School throughout the whole period the student is enrolled at the School.

The purposes for which School uses personal information of students and Parents include:
- to keep Parents informed about matters related to their child's schooling through correspondence, newsletters and magazines;
- day to day administration;
- looking after students' educational, social, spiritual and medical well-being;

- seeking donations and marketing for the School;
- seeking feedback from students and parents on school performance and improvement, including through school improvement surveys; and
- to satisfy the School legal obligations and allow the school to discharge its duty of care.

In some cases where the School requests personal information about a student or Parent, if the information requested is not obtained, the School may not be able to enrol or continue the enrolment of the student or permit the student to take part in a particular activity.

Job applicants, staff members and contractors
In relation to the personal information of job applicants, staff members and contractors, the School's primary purpose of collection is to assess and (if successful) engage the applicant, staff member or contractor, as the case may be.

The purposes for which the School use personal information of job applicants, staff members and contractors include:
- in administering the individual's employment or contract, as the case may be;
- for insurance purposes;
- seeking funds and marketing for the School; and
- to satisfy the School's legal obligations, for example, in relation to child protection legislation.

Volunteers
The School also obtains personal information about volunteers who assist the school in its functions or conduct associated activities, such as alumni associations, to enable the School and the volunteers to work together, to confirm their suitability and to manage their visits.

Marketing and fundraising
The School treats marketing and seeking donations for the future growth and development of the School as an important part of ensuring that the school continues to be a quality learning environment in which students and staff thrive. Personal information held by the School may be disclosed to an organisation that assists in the School fundraising, for example, an alumni organisation, church and parish authorities or the Catholic Archdiocese of Melbourne.

Parents, staff, contractors and other members of the wider school authority may from time to time receive fundraising information. The School publications, like newspapers and magazines, which include personal information, may be used for marketing purposes.

Who might the School disclose personal information to and store information with?

The School may disclose personal information, including sensitive information, held about an individual for educational, administrative and support purposes. This may include to:
- School service providers which provide educational, support and health services to the School, (either at the School or off campus) including the Catholic Education Commission of Victoria Ltd (CECV), Catholic Education Offices, specialist visiting teachers, volunteers, counsellors, sports coaches and providers of learning and assessment tools
- third party service providers that provide online educational and assessment support services, services in relation to school improvement surveys, document and data management services, or applications to schools and school systems including the Integrated Catholic Online Network (ICON) and Google's G Suite, including Gmail and, where necessary, to support the training of selected staff in the use of these services
- CECV and Catholic Education offices to discharge its responsibilities under the **Australian Education Regulation 2013 (Regulation)** and the **Australian Education Act 2013 (Cth)** (AE Act) relating to students with a disability.
- other third parties which the school uses to support or enhance the educational or pastoral care services for its students or to facilitate communications with Parents
- another school including to its teachers to facilitate the transfer of a student
- Federal and State government departments and agencies
- health service providers
- recipients of School publications, such as newsletters and magazines
- student's parents or guardians and their emergency contacts
- assessment and educational authorities including the Australian Curriculum, Assessment and Reporting Authority
- anyone you authorise the School to disclose information to
- anyone who we are required or authorised to disclose the information to by law, including child protection laws.

Nationally Consistent Collection of Data on school students with disability
The school is required by the Federal **Australian Education Regulation (2013)** and **Australian Education Act 2013 (Cth)** (AE Act) to collect and disclose certain information under the Nationally Consistent Collection of Data (NCCD) on students with a disability. The school provides the required information at an individual student level to the Catholic Education Offices and the CECV, as an approved authority. Approved authorities must comply with reporting, record keeping and data quality assurance obligations under the NCCD. Student information provided to the federal government for the purpose of the NCCD does not explicitly identify any student.

Sending and storing information overseas
The School may disclose personal information about an individual to overseas recipients, for instance, when storing personal information with 'cloud' service providers which are situated outside Australia or to facilitate a school exchange. However, the School will not send personal information about an individual outside Australia without:
- obtaining the consent of the individual (in some cases the consent will be implied); or
- otherwise complying with the Australian Privacy Principles or other applicable privacy legislation.

The School may from time to time use the services of third party online service providers (including for the delivery of services and third party online applications, or Apps relating to email, instant messaging and education and assessment, such as Google's G Suite, including Gmail) which may be accessible by you. Some personal information [including sensitive information] may be collected and processed or stored by these providers in connection with these services. These online service providers may be located in or outside Australia.

School personnel and the school's service providers, and the CECV and its service providers, may have the ability to access, monitor, use or disclose emails, communications (e.g. instant messaging), documents and associated administrative data for the purposes of administering the system and services ensuring their proper use.

The school makes reasonable efforts to be satisfied about the security of any personal information that

may be collected, processed and stored outside Australia, in connection with any cloud and third party services and will endeavour to ensure the cloud is located in countries with substantially similar protections as the APPs.

The countries in which the servers of cloud service providers and other third party service providers are located may include United States of America and the United Kingdom.

Where personal and sensitive information is retained by a cloud service provider on behalf of CECV to facilitate Human Resources and staff administrative support, this information may be stored on servers located in or outside Australia.

How does the School treat sensitive information?

In referring to 'sensitive information', the School means: information relating to a person's racial or ethnic origin, political opinions, religion, trade union or other professional or trade association membership, philosophical beliefs, sexual orientation or practices or criminal record, that is also personal information; health information and biometric information about an individual.

Sensitive information will be used and disclosed only for the purpose for which it was provided or a directly related secondary purpose, unless you agree otherwise, or the use or disclosure of sensitive information is allowed by law.

Management and security of personal information

The School's staff are required to respect the confidentiality of students' and Parents' personal information and the privacy of individuals.

The School has in place steps to protect the personal information the School holds from misuse, interference and loss, unauthorised access, modification or disclosure by use of various methods including locked storage of paper records and password access rights to computerised records. This includes responding to any incidents which may affect the security of the personal information it holds. If we assess that anyone whose information is affected by such a breach is likely to suffer serious harm as a result, we will notify them and the Office of the Australian Information Commissioner of the breach. Refer to the data breach section below.

It is recommended that parents and the school community adopt secure practices to protect themselves. You should ensure that all passwords you use are strong and regularly updated and that your log in details are kept secure. Do not share your personal information with anyone without first verifying their identity and organisation. If you believe any of your personal information has been compromised, please let the School know immediately.

Access and correction of personal information

Under the **Privacy Act 1988 (Cth)** and the **Health Records Act** an individual has the right to obtain access to any personal information which the School holds about them and to advise the School of any perceived inaccuracy. There are some exceptions to this right set out in the Act.

Students will generally be able to access and update their personal information through their Parents, but older students may seek access and correction themselves.

There are some exceptions to these rights set out in the applicable legislation.

To make a request to access or update any personal information that the School holds about you or your child, please contact the school's Principal in writing.

The School may require you to verify your identity and specify what information you require. The School may charge a fee to cover the cost of verifying your application and locating, retrieving, reviewing and copying any material requested. If the information sought is extensive, the School will advise the likely cost in advance. If we cannot provide you with access to that information, we will provide you with written notice explaining the reasons for refusal.

Consent and rights of access to the personal information of students

The School respects every Parent's right to make decisions concerning their child's education.

Generally, the school will refer any requests for consent and notices in relation to the personal information of a student to the student's Parents. The School will treat consent given by Parents as consent given on behalf of the student, and notice to Parents will act as notice given to the student.

As mentioned above, Parents may seek access to personal information held by the School about them or their child by contacting the school's Principal. However, there will be occasions when access is denied. Such occasions would include where the release of the information would have an unreasonable impact on the privacy of others, or where the release may result in a breach of the School duty of care to the student.

The School may, at its discretion, on the request of a student grant that student access to information held by the School about them, or allow a student to give or withhold consent to the use of their personal information, independently of their Parents. This would normally be done only when the maturity of the student and/or the student's personal circumstances so warranted.

How the School will manage an actual or suspected data breach under this policy

The School will manage the process of dealing with an actual or suspected breach in accordance with the **Data Breach Response Procedure**.

Enquiries and complaints

If you would like further information about the way the School manages the personal information it holds, or wish to make a complaint that you believe that the School has breached the Australian Privacy Principles, please contact the School Principal.

The School will investigate any complaint and will notify you of a decision in relation to your complaint as soon as is practicable after it has been made.

Implementation

This policy is implemented through a combination of:
- Staff training;
- Effective communication with the School community;
- Effective record keeping procedures; and
- Initiation of corrective actions where necessary.

Key Legislation and References

Privacy Act (Cth) 1988
Australian Privacy Principles
Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth)
Privacy Amendment (Notifiable Data Breaches) Act 2017

Related Policies

Data Breach Response Procedure

Review Date	August 2022, or upon each change in legislation or reference document.
Responsible Officer	Privacy Officer
Ratified by	School Principal and School Advisory Board
Policy last updated:	**Policy last updated on: September 2018 (CompliSpace implementation)**