HOPEPOINT
CHRISTIAN SCHOOL

# Privacy Policy

AUTHORISED BY:
Joe Britton
Principal

HOPEPOINT
CHRISTIAN SCHOOL

# Privacy Policy

## 1. Introduction

This statement outlines our school's policy on how it uses and manages personal information provided to or collected by it.

The School is bound by the National Privacy Principles contained in the Commonwealth Privacy Act.
The School 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 make sure it remains appropriate to the changing school environment.

## 2. Collection of personal information

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

- pupils and parents and/or guardians ('Parents') before, during and after the course of a pupil's enrolment at the School;
- job applicants, staff members, volunteers and contractors; and
- other people who come into 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 pupils, face-to-face meetings and interviews, and telephone calls. On occasions people other than Parents and pupils provide personal information.

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.

Exception in relation to employee records: Under the Privacy Act the National 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 employee.

## 3. How the School uses collected information

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 to which you have consented.

Pupils and Parents: In relation to personal information of pupils and Parents, the School's primary purpose of collection is to enable the School to provide schooling for the pupil. This includes satisfying both the needs of Parents and the needs of the pupil throughout the whole period the pupil is enrolled at the School.

The purposes for which the School uses personal information of pupils 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 pupils' educational, social and medical wellbeing;
- seeking donations and marketing for the School;
- to satisfy the School's legal obligations and allow the School to discharge its duty of care.

In some cases where the School requests personal information about a pupil or Parent, if the information requested is not obtained, the School may not be able to enrol or continue the enrolment of the pupil.

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

The purposes for which the School uses 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;
- 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.

Who might the School disclose personal information to?
The School may disclose personal information, including sensitive information, held about an individual to:

- another school;
- government departments;
- medical practitioners;
- people providing services to the School, including specialist visiting teachers and sports coaches;
- recipients of School publications, like newsletters and magazines;
- Parents; and anyone you authorise the School to disclose information to.

*Sending information overseas:* The School will not send personal information about an individual outside Australia without:

- obtaining the consent of the individual (in some cases this consent will be implied); or
- otherwise complying with the National Privacy Principles.

## 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, sexual preferences or criminal record, that is also personal information; and health 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 the sensitive information is allowed by law.

**Management and security of personal information**
The School's staff are required to respect the confidentiality of pupils' 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, loss, unauthorised access, modification or disclosure by use of various methods including locked storage of paper records and pass worded access rights to computerised records.

**Management and security of student photos/videos**
Collection

- **Principle 1 – Lawful**
  Only collect personal information for a lawful purpose, which is directly related to the Office's activities and necessary for that purpose

- **Principle 2 – Direct**
  Only collect personal information directly from the person concerned, unless it is unreasonable or impracticable to do so

- **Principle 3 – Open**
  Inform the person why you are collecting personal information, what you will do with it and who else might see it. Tell the person how they can view and correct their personal information and any consequences that may apply if they decide not to provide their information to you.

- **Principle 4 – Relevant**
  Ensure that the personal information is relevant, accurate, not excessive and up-to-date and that the collection does not unreasonably intrude into the personal affairs of the individual.

Storage

- **Principle 5 – Secure**
  Store personal information securely; keep it no longer than necessary and dispose of it appropriately. It should also be protected from unauthorised access, use or disclosure.

Access and accuracy

- **Principle 6 – Transparent**
  Explain to the person what personal information about them is being stored, why it is being used and any rights they have to access it.

- **Principle 7 – Accessible**
  Allow people to access their personal information without unreasonable delay or expense.

- **Principle 8 – Correct**
  Allow people to update, correct or amend their personal information where necessary.

Use

- **Principle 9 – Accurate**
  Make sure that the personal information is relevant and accurate before using it.

- **Principle 10 – Limited**
  Only use personal information if the person has given their consent or if they were informed at the time of collection.

Disclosure

- **Principle 11 – Restricted**
  Only disclose personal information with a person's consent or if the person was told at the time that it would be disclosed. Personal information can be used without a person's consent in order to deal with a serious and imminent threat to any person's health or safety.

- **Principle 12 – Safeguarded**
  An agency cannot disclose sensitive personal information without a person's consent; for example, information about ethnic or racial origin, political opinions, religious or philosophical beliefs, health or sexual activities or trade union membership. It can only disclose sensitive information without consent in order to deal with a serious and imminent threat to any person's health or safety.

Exemptions to the IPPs

If a public sector agency believes that the information protection principles are unworkable in a particular circumstance, it can either make a Privacy Code of Practice or seek an exemption from, or modification to, the principle from the Privacy Commissioner.

Privacy Codes of Practice allow an agency to modify one or more of the information protection principles. Codes of Practice can be made in relation to one of three things:

- a particular type of personal information (s29(5)(a))
- a particular organisation or type of organisation (s29(5)(b))
- a type of activity (s29(5)(c)).

A Privacy Code of Practice can change or delete any of the information protection principles but it cannot change or delete any of the exceptions to the principles, nor can it increase the level of privacy protection above that of the information protection principles.

Offences

Offences can be found in s62–66 of the PPIP Act. It is an offence for the OBOS to:

- intentionally disclose or use personal information accessed in doing our jobs for an authorised purpose
- offer to supply personal information that has been disclosed unlawfully
- hinder the Privacy Commissioner or a member of staff from doing their job.

The HRIP Act and Health Information

The HRIP Act sets out how the OBOS must manage **health** information.

*About health information*:

Health information is a more specific type of personal information and is defined in s6 of the HRIP Act. Health information can include information about a person's physical or mental health such as a psychological report, blood tests or an X-ray, or even information about a person's medical appointment. It can also include some personal information that is collected to provide a health service, such as a name and contact number on a medical record.

Health Privacy Principles (HPPs)

Schedule 1 to the HRIP Act contains 15 HPPs that we must comply with. Here is an overview of them as they apply to us:

Collection

**Principle 1 – Lawful**

An agency or organisation can only collect your health information for a lawful purpose. It must also be directly related to the agency or organisation's activities and necessary for that purpose.

**Principle 2 – Relevant**

An agency or organisation must ensure that your health information is relevant, accurate, up-to-date and not excessive. The collection should not unreasonably intrude into your personal affairs.

**Principle 3 – Direct**

An agency or organisation must collect your health information directly from you, unless it is unreasonable or impracticable to do so.

**Principle 4 – Open**

An agency or organisation must inform you of why your health information is being collected, what will be done with it and who else might access it. You must also be told how you can access and correct your health information and any consequences if you decide not to provide it.

Storage

**Principle 5 – Secure**

An agency or organisation must store your personal information securely, keep it no longer than necessary and dispose of it appropriately. It should also be protected from unauthorised access, use or disclosure.

Access and accuracy

**Principle 6 – Transparent**

An agency or organisation must provide you with details regarding the health information they are storing, why they are storing it and what rights you have to access it.

**Principle 7 – Accessible**

An agency or organisation must allow you to access your health information without unreasonable delay or expense.

**Principle 8 – Correct**

An agency or organisation must allow you to update, correct or amend your health information where necessary.

**Principle 9 – Accurate**

An agency or organisation must make sure that your health information is relevant and accurate before using it.

Use

**Principle 10 – Limited**

An agency or organisation can only use your health information for the purpose for which it was collected, or a directly related purpose that you would expect (unless one of the exemptions in HPP 10 applies). Otherwise separate consent is required.

Disclosure

**Principle 11 – Restricted**

An agency or organisation can only disclose your health information for the purpose for which it was collected or a directly related purpose that you would expect (unless one of the exemptions in HPP 11 applies). Otherwise separate consent is required.

Identifiers and anonymity

**Principle 12 – Not identified**

An agency or organisation can only give you an identification number if it is reasonably necessary to carry out their functions efficiently.

**Principle 13 – Anonymous**

You are entitled to receive health services anonymously, where this is lawful and practicable.

Transferrals and linkage

**Principle 14 – Controlled**

Your health information can only be transferred outside New South Wales in accordance with HPP 14.

**Principle 15 – Authorised**

Your health information can only be included in a system to link health records across more than one agency or organisation if you have consented.

Exemptions to the HPPs

Exemptions are located mainly in Schedule 1 to the HRIP Act, and may allow the OBOS not to comply with the HPPs in certain situations.

Health privacy codes of practice and public interest directions can modify the HPPs for any NSW public sector agency. All of these are available on the Privacy Commissioner's website.

Offences

Offences can be found in s68–70 of the HRIP Act. It is an offence for the OBOS to:

intentionally disclose or use health information accessed in doing our jobs for anything else other than what we are authorised to

offer to supply health information that has been disclosed unlawfully

attempt to persuade a person from making or pursuing a request for health information, a complaint to the Privacy Commissioner or an internal review under the PPIP Act.

Other laws that affect how we comply with the IPPS and HPPS

This section contains information about the main laws that affect how the OBOS complies with the IPPs and HPPs.

*Education Act 1990* and regulations

*Government Information (Public Access) Act 2009* (GIPA Act)

*Crimes Act 1900*

*ICAC Act 1988*

*Public Interest Disclosures Act 1994*

*State Records Act 1998* and regulations.

The following policies and procedures support compliance with the Act:

NSW Government Personnel Handbook issued by the Public Service Commission;

Privacy Code of Practice for the NSW Public Sector Workforce Profile, Department of Premier and Cabinet;

State Records Authority of NSW, Government Recordkeeping Manual;

Office of the Board of Studies Code of Conduct and Ethics – This code of conduct establishes standards of professional behaviour expected of staff of the Office. The code was developed to

assist all officers in clarifying their professional and ethical responsibilities in executing their duties, thereby encouraging public confidence in the work of the Board and its Office.

Use of Office Communications Devices Policy –This policy statement sets out the principles underpinning the use of Office communication devices. The policy covers the responsibilities of all staff in relation to economy, personal use, record keeping, security and privacy, and unlawful use.

Records Management Policy **–** This policy provides a basis for the effective management of the records generated by the Office, which in turn are assets of New South Wales. The policy is designed to inform staff about their responsibilities in relation to the creation, control, management, preservation and disposal of official records in all mediums.

Security of Electronic Information Systems Policy – The Office holds a considerable amount of data in its various computer systems, much of which is confidential and sensitive. This Policy, and its accompanying procedures and materials, address all aspects of security relating to the Office's systems. It sets out the principles held by the Office regarding security, identifies responsibilities of staff, and outlines the Office's procedures in a wide range of areas.

Updating personal information

The School endeavours to ensure that the personal information it holds is accurate, complete and up-to-date. A person may seek to update their personal information held by the School by contacting the school office at any time.

The National Privacy Principles require the School not to store personal information longer than necessary.

You have the right to check what personal information the School holds about you

Under the Commonwealth Privacy 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. Pupils will generally have access to their personal information through their Parents, but older pupils may seek access themselves.

To make a request to access any information the School holds about you or your child, please contact the 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.

Consent and rights of access to the personal information of pupils

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 pupil to the pupil's Parents. The School will treat consent given by Parents as consent given on behalf of the pupil, and notice to Parents will act as notice given to the pupil.
Parents may seek access to personal information held by the School about them or their child by contacting the Principal. However, there will be occasions when access is denied. Such occasions would include where 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's duty of care to the pupil.
The School may, at its discretion, on the request of a pupil grant that pupil access to information held by the School about them, or allow a pupil 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 pupil and/or the pupil's personal circumstances so warranted.

Enquiries
If you would like further information about the way the School manages the personal information it holds, please contact the school office.