Date last approved	June 2018
Frequency of reviews	Every 2 years
Next review due	June 2020
Audience	All staff
Stakeholders	Principal, Executive, All staff

Contents

1. Introduction

1.1. Overview

The College is required to protect the privacy of individuals when it handles their personal information. This policy covers the responsibilities of both the College and employees in relation to privacy.

1.2. Rationale

The College is required to comply with the *Privacy Act 1988* (the Act) as they have a turnover of greater than $3 million. This policy summarises the College's responsibilities under the Act.

1.3. Key concepts

Australian Privacy Principles

The Act includes thirteen Australian Privacy Principles (APPs) which list the standards, rights and obligations for how personal information can be collected and used. The APPs are summarised in this policy.

Office of the Australian Information Commissioner (OAIC)

The Office of the Australian Information Commissioner (OAIC) is responsible for overseeing the Privacy Act, including handling complaints, conducting investigations and providing advice.

1.4. Penalties

If the College breaches someone's privacy they can be required to compensate that person for loss or damage (including injury to their feelings or humiliation).

The maximum penalty for serious or repeated interferences with privacy is $2.1 million[1].

The College may also be liable to pay a penalty if it (or one of its Directors, employees or agents) attempts to, induces, conspires or is knowingly concerned in the contravention of the Act, unless the College can show it took reasonable precautions and exercised due diligence to avoid this happening.

The most significant consequence for the College for a breach of privacy is the loss of reputation. In addition to being required to notify all people affected by the breach and the Australian Information Commissioner, breaches that are investigated become a permanent record on the OAIC website, available to anyone, including the media.

[1] *2,000 penalty units x $210 per unit x 5 times, as per Section 13G and Section 80W of the Act*

2. Definitions

2.1. Personal information

The Act defines personal information in Section 6 as follows:

> Personal information is **information or an opinion** about an **identified individual**, or an **individual who is reasonably identifiable**:
>
> (a) whether the information or opinion is **true or not**; and
> (b) whether the information or opinion is recorded in a **material form or not**.

It is important to note that personal information can be:

- Information or an opinion
- True or not
- Recorded in material form or not

Also, even if the information does not include a person's name, if the person can be reasonably identified by the rest of the information, it is still considered personal information.

Examples of personal information at the College can include the following information about students, parents, staff members, job applicants or contractors:

- Name
- Signature
- Address
- Phone number
- Date of birth
- Medical records
- Bank account details
- Commentary or an opinion about that person

2.2. Sensitive information

A type of personal information that requires even stricter controls is sensitive information[2]. As defined by the Act in Section 6, sensitive information can include **information or an opinion** about an individual's:

- Racial or ethnic origin
- Political opinions or membership of a political association
- Religious beliefs or affiliations, or philosophical beliefs
- Membership of a professional or trade association, or membership of a trade union
- Sexual orientation or practices
- Criminal record
- Health

[2] *See APP 3, APP 6 and APP 7 in the Act*

3. College responsibilities

3.1. Australian Privacy Principles

The College is committed to fulfilling its privacy responsibilities as listed in the Australian Privacy Principles (APPs). A summary[3] of how these APPs apply to the College is outlined in the policy statements below:

Principle	Policy Statements
APP 1 | Open and transparent management of personal information	• The College will implement systems and procedures to ensure the College complies with the APPs including: - Arrangements for who is responsible for managing privacy - Processes for the handling of personal information - Processes for dealing with inquiries or complaints from individuals about the College's compliance with the APPs - Training for staff - A *Data Breach Response Plan* • The College will have an up-to-date and clear *APP Privacy Policy* (see Appendix A) that outlines the College's general information handling practices on the College website.
APP 2 | Anonymity and pseudonymity	• The College will give individuals the option of not identifying themselves or using a pseudonym when dealing with the College, unless they are required by law to identify themselves or it is not practical for the College to deal with them unless they identify themselves.
APP 3 | Collection of solicited personal information	The College: • Will not collect personal information unless it is reasonably necessary for the College's functions and activities. • Will not collect sensitive information unless the individual has consented[4] to the collection of information and that information is reasonably necessary for the College's functions and activities, unless it is permitted in the Act (e.g. to lessen or prevent a threat to health, safety or life of a person). • Will only solicit and collect personal information by lawful and fair means, and directly from the individual, unless it is unreasonable or impracticable to do so.
APP 4 | Dealing with unsolicited personal information	• If someone accidentally and unintentionally provides personal information to the College, the College will destroy or de-identify it as soon as possible (unless it is unlawful or unreasonable to do so). • Any personal information intentionally provided to the College will be handled in accordance with the APPs.
APP 5 | Notification of the collection of personal information	• Before, at the time of, or as soon as possible after collecting personal information from a person, the College will ensure the person is aware of how the College will handle the information (e.g. by providing a *Collection Notice*[5]).

[3] *A more detailed summary of these requirements is listed in the* Privacy Procedures.

[4] *Unless it is unreasonable or impractical to do so (e.g. for younger students, in which case you would gain their parent's approval).*

[5] *Collection Notices are in an Appendix of the* Privacy Procedures.

Principle	Policy Statements
APP 6 | Use or disclosure of personal information	• The College will only use or disclose personal information for the purpose for which it was collected, unless they are permitted to use it for another purpose under the Act.
APP 7 | Direct Marketing	• The College will not use the personal or sensitive information it has collected for direct marketing, unless it has met the requirements under the Act (e.g. the person has consented to direct marketing and the College clearly provides a simple way for the person to 'opt out'). • The College will never sell personal information it collects to third parties.
APP 8 | Cross border disclosure of personal information	• The College is accountable for any breaches of the APPs by the overseas recipient. Therefore, the College will not disclose personal information to an overseas recipient (including providers of digital services) unless one of the following applies: - The College has taken reasonable steps to ensure the overseas recipient does not breach the APPs. - The College reasonably believes that the overseas recipient is subject to a law substantially similar to the APPs and the College can take action to enforce that law or scheme. - The College expressly informs the person that the College is not responsible for any breaches of personal information and the person consents to the disclosure. - The College is permitted to do so in the Act (e.g. to lessen or prevent a threat to health, safety or life of a person).
APP 9 | Adoption, use or disclosure of government related identifiers	• The College will not use government related identifiers (e.g. Tax File Number, Medicare Number, Centrelink Number) as its own identifier. • The College will not use or disclose government related identifiers unless it is permitted to do so in the Act (e.g. to lessen or prevent a threat to health, safety or life of a person).
APP 10 | Quality of personal information	• The College will take reasonable steps to ensure the information it collects, uses and discloses is accurate, up-to-date, complete and relevant.
APP 11 | Security of personal information	• The College will take reasonable steps to protect personal information from misuse, interference, loss and unauthorised access, modification or disclosure • Once personal information is no longer required for a purpose allowed by the Act or required to be retained by Australian law, the College will destroy or de-identify the information[6].

[6] *See the 'Records Retention Schedule for Non-Government Schools from the Australian Society of Archivists Inc' for details of how long documents must be retained.*

Principle	Policy Statements
APP 12 | Access to personal information	• If requested, the College will give a person access to their personal information within a reasonable amount of time and in the manner requested by the individual as long as it's reasonable and practicable, unless an exception applies in the Act. The charge for giving access will not be excessive. • If access is denied, the College will give written notice to the person explaining the reasons for the refusal (unless it's unreasonable to do so) and how the person can complain about the refusal.
APP 13 | Correction of personal information	• If the College becomes aware that personal information is inaccurate, out of date, incomplete, irrelevant or misleading, or if the person requests that the College correct the information, the College will correct the information, notifying any third parties who received that information from the College (unless it is impracticable or unlawful to do so). • If a request for correction is refused, the College will give a written notice to the person explaining the reasons for the refusal (unless it would be unreasonable to do so) and how the person can complain about the refusal. • The College will respond to these requests within a reasonable amount of time and will not charge the individual for any of these actions.

3.2. Tax File Numbers

Under *Privacy (Tax File Number) Rule 2015*, the College is required to protect the privacy of an individual's Tax File Number (TFN). There are significant penalties if this privacy is not protected. A summary[7] of how these requirements apply to the College is outlined in the policy statements below:

- The College will not use TFNs as their identification numbers.
- The College will only request, collect, use or disclose TFNs for a purpose authorised by taxation law, personal assistance law or superannuation law.
- The College will take reasonable steps when requesting a TFN to make sure:
  - The person is informed of the law that authorises the collection of their TFN and the purpose for which the TFN is being requested.
  - The person is informed that it's not an offence to not provide their TFN but what the consequences will be for declining to provide it.
  - The way it is collected does not unreasonably intrude on the individual's affairs.
- The College will take reasonable steps to protect TFN information from misuse, loss, unauthorised access, use, modification or disclosure, and ensure that access to TFN records are restricted to those who need it for purposes authorised by taxation law, personal assistance law or superannuation law.
- The College will take reasonable steps to securely destroy or permanently de-identify TFN information when it is no longer required to be retained by law or no longer required for purposes authorised by taxation law, personal assistance law or superannuation law.
- The College will provide training:
  - To **all staff** on the need to protect the privacy of individuals when handling TFN information.
  - To **all staff who collect or access TFN information** on when TFN information may be collected, the rules around the use and disclosure of TFN information and the penalties for breaking these rules

[7] *A more detailed summary of these requirements is listed in the* Privacy Procedures.

3.3. Privacy Impact Assessments

When the College implements a new project that will involve the collection, use or disclosure of personal information, it will conduct a Privacy Impact Assessment (PIA)[8] to ensure the project complies with the APPs. This PIA will vary in size and scope, depending on the type of project.

3.4. ICT security requirements

To secure personal information that is stored electronically[9], the ICT Department is responsible for ensuring that:

- All software used by the College is reviewed regularly so that it is sufficiently secure (this includes ensuring that the latest versions, patches and security updates are installed).
- Encryption is used to ensure information is stored in a way that it can't be easily understood by unauthorised individuals.
- Appropriate security controls are in place to protect the network (e.g. firewalls, monitoring the network activities, filters).
- An intrusion prevention and detection system is employed and maintained, and event logs are regularly analysed.
- Regular backups are made of all important files and those backups are stored off-site in a secure location.
- Access to electronic files is limited to those who require it for their work.
- Systems are in place to ensure:
  - Network users must be authenticated (e.g. through a username and password).
  - Passwords are sufficiently complex.
  - Users are locked out after a specified number of failed logins.
  - Screen lock programs are activated when devices are not in use.
- Audit logs and audit trails are used to identify inappropriate access of files or databases containing personal information.
- Systems are in place to manage the secure transmission of personal information via email and staff are informed of these systems.
- Where third party network, software and/or storage providers are used by the College, their security controls and personal information handling measures are assessed to ensure they comply with the APPs.
- Backups are regularly reviewed to ensure that personal information that is no longer required is destroyed or de-identified.
- The operation and effectiveness of ICT security measures are regularly monitored to ensure that they remain responsive to changing threats, vulnerabilities and other issues that may impact the security of personal information.

---

[8] For a very detailed explanation of how to conduct a PIA see the OAIC website: https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-undertaking-privacy-impact-assessments

[9] More information about securing personal information that is stored electronically can be found in the OAIC document, Guide to securing personal information.

3.5. Employee records

As per Section 7B(3) of the Act, the handling of an employee's personal information by the College is exempt from the Privacy Act if it is directly related to:

- Their current or former employment relationship
- The employee's record

This means the College does not need to comply with the APPs when it handles current and past employee records for something that is directly related to the employment relationship. This also means that the College does not have to grant employees access to their employee records under the Privacy Act.

3.6. Data breaches

Notifiable Data Breaches Scheme (NDBS)

The College has responsibilities under the Notifiable Data Breaches Scheme (NDBS), which states that the College must notify the Commissioner and the individuals affected if:

- A data breach occurs involving personal information AND
- That personal information is likely to result in serious harm to any individual affected AND
- The College has not been able to prevent the likely risk of serious harm with remedial action

Data Breach Response Plan

The College will have a Data Breach Response Plan to meet its obligations under the Privacy Act and to limit the consequences of a data breach. This Response Plan will include:

- What constitutes a data breach
- Strategies for containing, assessing and managing data breaches
- Roles and responsibilities for staff in the event of a data breach
- How to notify the Commissioner and affected individuals if there is a likelihood that the data breach could cause serious harm
- How data breaches will be documented
- A review of how the breach occurred, how it was managed and what changes need to be made for the future

4. Employee responsibilities

All employees are responsible for ensuring that they:

- Only collect, use, access and disclose personal information that is reasonably required for them to do for their work.
- Discuss appropriate protocols with their line manager if they need to handle personal information relating to a person known to them (e.g. a close friend or relative) and, where possible, refer this task to another employee.
- Authenticate an individual's identity before disclosing personal information.
- Protect personal information from misuse, interference, loss, unauthorised access, modification or disclosure by using appropriate security measures (e.g. password protection, locked filing cabinets).
- Maintain confidentiality when discussing personal information with other staff (e.g. only discussing with those who need to know, conducting discussions in private spaces).
- Avoid taking personal information off the College grounds unless it is approved by their line manager and they are able to do so in a secure manner.
- Record personal information in a factual, objective manner.
- Destroy all documentation containing personal information that is no longer needed in the blue confidential bin (unless it needs to be retained under the *Records Retention Schedule for Non-Government Schools*).
- Ensure information is de-identified before it is publicly reported, unless approval has been given to identify the individuals involved.
- Notify their line manager or the Privacy Officer immediately if they think they may have breached an individual's privacy.

More detailed information about how employees can fulfil their responsibilities is contained in the *Privacy Procedures*.

5. Privacy Officer responsibilities

The Privacy Officer is responsible for:

- Keeping up to date with the Privacy legislation and best practice, advising the Executive of any changes.
- Monitoring the implementation of this policy and providing feedback to the Executive if they observe staff not complying with the policy.
- Providing advice to the Executive and staff about privacy matters.
- Reviewing the Privacy Policy every three years.

If appropriate, the Privacy Officer can request the formation of a Privacy Committee to help them outwork these responsibilities.

6. Supporting information

6.1. Procedure and forms

There are no procedures or forms associated with this Policy.

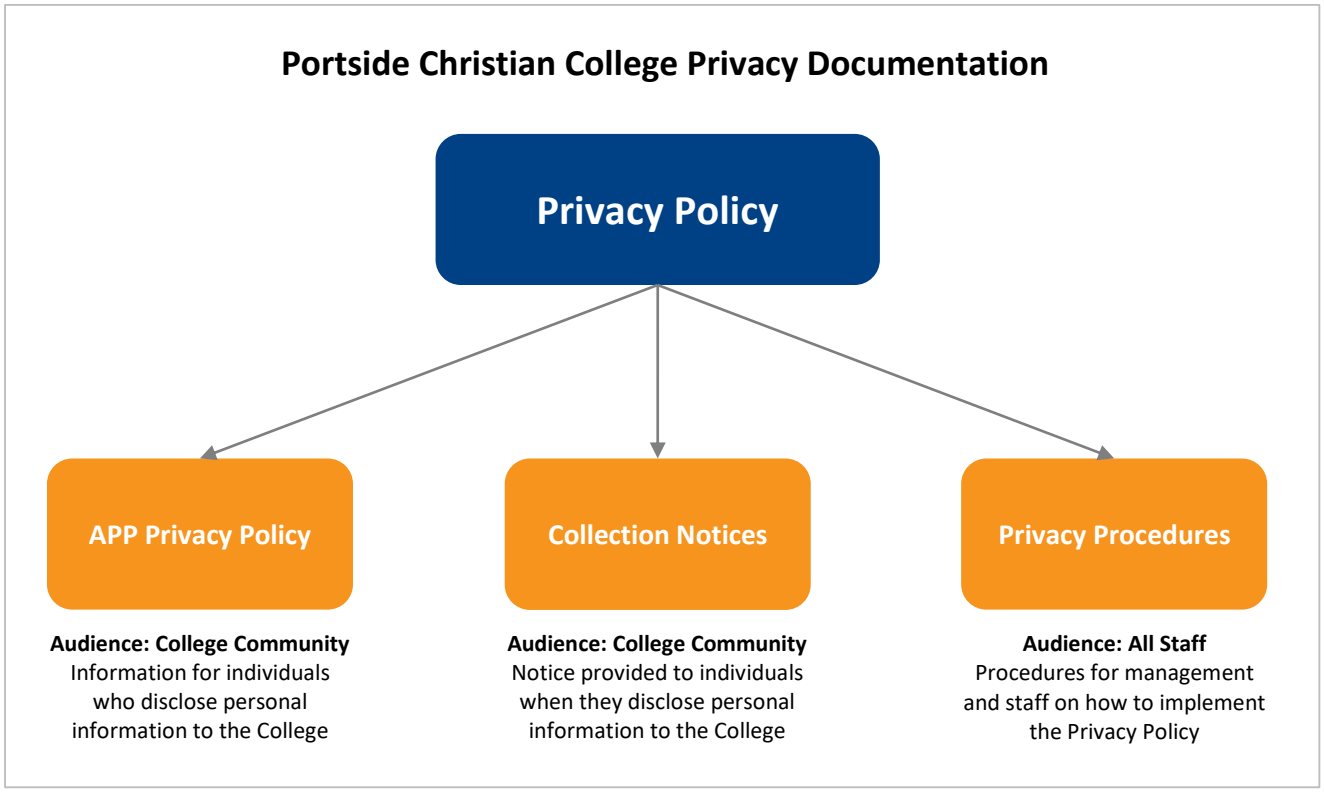
6.2. Child protection

Note any implications this policy has for child protection.

6.3. Related documents

The following documents should be read in conjunction with this policy:

- APP Privacy Policy
- Collection Notices (Appendix in the Privacy Procedures)
- Privacy Procedures (includes a Data Breach Response Plan)



In addition, the *Records Retention Schedule for Non-Government Schools from the Australian Society of Archivists Inc* provides information about how long documents must be retained before they can be destroyed.

6.4. Legislation/regulations

The following legislation/regulations are relevant to or impact on this policy:

- Privacy Act 1988
- Privacy (Tax File Number) Rule 2015

6.5. References

The following resources from the Office of the Australian Information Commissioner (OAIC) were referenced:

- Privacy Management Framework, https://www.oaic.gov.au/agencies-and-organisations/guides/privacy-management-framework
- Guide to developing an APP privacy policy, https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-developing-an-app-privacy-policy
- Guide to securing personal information, https://www.oaic.gov.au/resources/agencies-and-organisations/guides/guide-to-securing-personal-information.pdf
- Notifiable Data Breaches Scheme, https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme
- Data Breach Preparation and Response, https://www.oaic.gov.au/resources/agencies-and-organisations/guides/data-breach-preparation-and-response.pdf
- Privacy business resource 9: Ten tips to protect your customers' personal information, https://www.oaic.gov.au/agencies-and-organisations/business-resources/privacy-business-resource-9
- Guide to undertaking privacy impact assessments, https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-undertaking-privacy-impact-assessments
- Guide to information security: 'reasonable steps' to protect personal information, https://www.oaic.gov.au/images/documents/privacy/privacy-guides/information-security-guide-2013_WEB.pdf

6.6. Policy dissemination and training

Dissemination/Training	Who	Frequency
Group or one-on-one training on: • Privacy Policy • Privacy Procedures	All staff	• When policy first approved • On commencement (new staff) • A refresher every 3 years
Group or one-on-one training on: • Protection of TFNs (part of the Privacy Procedures)	Administration staff	• When policy first approved • On commencement (new staff) • A refresher every 3 years
Group or one-on-one training on: • Data Breach Response Plan (part of the Privacy Procedures)	Executive members Heads of Schools	• When policy first approved • On commencement (new staff) • A refresher every 3 years
A brief overview of the Privacy Policy and Privacy Procedures at a Staff Meeting	All staff	• Once every year (excluding the years when group training is conducted)
A reminder of the College's APP Privacy Policy in the College Newsletter	College community	• Once every year

6.7. Distribution

Information from this policy should be included in the following documents:

☒ College Handbook
☒ Staff Handbook
☒ ELC Handbook
☒ OSHC Handbook

6.8. Change history

Review Date	Amendments
2014	• Policy first drafted
1 June 2018	• Comprehensive changes including legislative updates.

Appendix A – APP Privacy Policy

Overview

This *APP Privacy Policy* sets out how Portside Christian College (the College) manages personal information provided to or collected by it. The College is bound by the Australian Privacy Principles (APPs) contained in the Commonwealth Privacy Act 1988 (the Act).

The College will review and update this *APP Privacy Policy* periodically to take account of new laws and technology, changes to the College's operations and practices, and to make sure it remains appropriate to the changing school environment.

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

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

- students and parents/guardians (parents) before, during and after the course of a student's enrolment at the College, including:
  - name, contact details (including next of kin), date of birth, gender, language background, nationality, country of birth and previous school;
  - religion, church and referring pastor;
  - parents' education, occupation, language background, religion;
  - medical information (e.g. details of disability and/or allergies, absence notes, immunisation records, accident reports, medical certificates, medical reports, names of doctors, nutrition and dietary requirements, psychological reports);
  - conduct and complaint records, or other behaviour notes, and school reports;
  - information about referrals to government welfare agencies;
  - counselling reports;
  - health fund details and Medicare number;
  - custody details and any court orders;
  - correspondence with parents;
  - volunteering information; and
  - photos and videos at College events;
- job applicants, staff members, volunteers and contractors, including:
  - name, contact details (including next of kin), date of birth, residency status, religion, country of birth, nationality;
  - information on job application;
  - professional development history;
  - teacher registration number;
  - salary and payment information, including superannuation details and tax file number;
  - criminal record checks and working with children clearances;
  - medical information (e.g. details of disability and/or allergies, medical certificates, compensation claims);
  - complaint records and investigation reports;
  - leave details;
  - photos and videos at College events;
  - workplace surveillance information;
  - work emails and private emails (when using work email address) and Internet browsing history; and
- other people who come into contact with the College, including name and contact details and any other information necessary for the particular contact with the College.

Personal information you provide

The College 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 occasion people other than parents and students provide personal information.

Personal information provided by other people

In some circumstances the College 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.

How will the College use the personal information you provide?

The College 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 are reasonably expected by you, or to which you have consented.

Students and parents

In relation to personal information of students and parents, the College's primary purpose of collection is to enable the College to provide schooling to enrolled students, exercise its duty of care and perform necessary associated administrative activities which will enable students to take part in all the activities of the College. This includes satisfying the needs of parents, the needs of the student and the needs of the College throughout the whole period the student is enrolled at the College. The purposes for which the College 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 of the College;
- looking after students' educational, social, spiritual and medical wellbeing;
- seeking donations and marketing for the College;
- to refer unpaid debts to a debt collection agency;
- to contribute to aggregated data that Portside Christian College may require from time to time to meet its reporting, planning, contract and funding responsibilities; and
- to satisfy the College's legal obligations and allow the College to discharge its duty of care.

In some cases where the College requests personal information about a student or parent, if the information requested is not provided, the College 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 and contractors

In relation to personal information of job applicants and contractors, the College's primary purpose of collection is to assess and, if successful, engage the applicant or contractor. The purposes for which the College uses personal information of job applicants and contractors include:

- administering the individual's employment or contract;
- insurance purposes;
- seeking donations and marketing for the College; and
- contributing to aggregated data that Portside Christian College may require from time to time to meet its reporting, planning, contract and funding responsibilities;
- satisfying the College's legal obligations, for example, in relation to child protection legislation.

Volunteers

The College also obtains personal information about volunteers who assist the College in its functions or associated activities to enable the College and the volunteers to work together.

Marketing and fundraising

The College treats marketing and seeking donations for the future growth and development of the College as an important part of ensuring that the College continues to provide a quality learning environment in which both students and staff thrive. Personal information held by the College may be disclosed to organisations that assist in the College's fundraising such as an internal fundraising committee or external fundraising provider. The College will not disclose an individual’s personal information to third parties for their own marketing purposes without the individual’s consent.

Parents, staff, contractors and other members of the wider College community may from time to time receive fundraising information. Individuals may opt out of receiving marketing and promotional material from the College at any time by contacting the Privacy Officer (see contact details at end of policy). College publications, like newsletters and magazines, which include personal information, may be used for marketing purposes.

Who might the College disclose personal information to and store your information with?

The College may disclose personal information, including sensitive information, held about an individual for educational, administrative and support purposes. This may include to:

- students' parents;
- other schools and teachers at those schools;
- government departments (including for policy and funding purposes);
- medical practitioners;
- people providing educational, support and health services to the College (e.g. specialist visiting teachers, sports coaches, volunteers, consultants and counsellors);
- providers of specialist advisory services and assistance to the College, including in the areas of Human Resources, child protection and students with additional needs;
- providers of learning and assessment tools;
- assessment and educational authorities, including the Australian Curriculum, Assessment and Reporting Authority (ACARA) and NAPLAN Test Administration Authorities (who will disclose it to the entity that manages the online platform for NAPLAN);
- people providing administrative and financial services to the College;
- recipients of College publications, such as newsletters and magazines;
- Portlife Church staff;
- insurance companies;
- anyone you authorise the College to disclose information to; and
- anyone to whom the College is required or authorised to disclose the information to by law, including child protection laws.

Sometimes the College may ask individuals (either in writing or verbally) to consent to disclosure or use of personal information for certain purposes. In other cases, such as those listed above, consent may be implied.

Photographs and videos

Information such as academic and sporting achievements, student activities and similar news is sometimes published in College newsletters and magazines, on our intranet and on our website. This may include photographs and videos of student activities such as sporting events, camps and excursions. The College will obtain permissions annually from the student's parent (and from the student if appropriate) to include these photographs, videos or other identifying material in publicly available places (e.g. promotional materials, College website).

Overseas disclosure

The College may disclose personal information about an individual to overseas recipients, for example, to facilitate a school exchange or missions trip. However, the College 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 Australian Privacy Principles or other applicable privacy legislation.

The College may use online or cloud service providers to store personal information and to provide services to the College that involve the use of personal information, such as services relating to email, instant messaging and education and assessment applications. Some limited personal information may also be provided to these service providers to enable them to authenticate users that access their services. This personal information may be stored in the cloud which means that it may reside on the cloud service provider's servers which may be situated outside Australia.

An example of such a cloud service provider is Google. Google provides the *G Suite for Education* including Gmail, and stores and processes limited personal information for this purpose. College personnel and the AIS 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 *G Suite for Education* and ensuring its proper use.

How does the College treat sensitive information?

In referring to 'sensitive information', the College 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, criminal record, health information and biometric information.

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 is allowed by law.

How is personal information stored and secured?

The College stores personal information in a variety of ways including in physical files, on our network, and in online database and storage services. The security of your personal information is important, and the College has in place various measures to protect the personal information the College holds from misuse, interference and loss, unauthorised access, modification or disclosure including locked storage of paper records and password access rights to digital records.

How can I access and correct personal information?

Under the Act, an individual has the right to seek and obtain access to any personal information which the College holds about them and to advise the College of any perceived inaccuracy. 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 Act.

To make a request to access or update any personal information the College holds about you or your child, please contact the Privacy Officer (see contact details at end of policy). The College may require you to verify your identity and specify what information you require. The College 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 College will advise the likely cost in advance.

Access may be refused in certain circumstances such as where access would have an unreasonable impact on the privacy of others, where access may result in a breach of the College's duty of care to the student, or where students have provided information in confidence. If access is refused you will be provided with written notice explaining the reasons for refusal.

Consent and rights of access to the personal information of students

The College respects every parent's right to make decisions concerning their child's education.

Generally, the College will refer any requests for consent and notices in relation to the personal information of a student to the student's parents. The College 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.

Parents may seek access to personal information held by the College about them or their child by contacting the Privacy Officer (see contact details at end of policy). However, there may 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 College's duty of care to the student.

The College may, at its discretion, on the request of a student grant that student access to information held by the College 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 warrant it.

Exemption in relation to employee records

Under the Act, the Australian Privacy Principles do not apply to an employee record. As a result, this APP Privacy Policy does not apply to the College's treatment of an employee record, where the treatment is directly related to a current or former employment relationship between the College and employee.

Enquiries and complaints

If you would like further information about how the College manages the personal information it holds or wish to complain because you believe that the College has breached the APPs please contact the Privacy Officer (see contact details below). The College will investigate any complaint and will notify you of the decision in relation to your complaint as soon as is practicable.

Contact Details

For more information contact the Privacy Officer:

1 Causeway Rd
NEW PORT SA 5015
(08) 8341 5133
admin@portside.sa.edu.au
www.portside.sa.edu.au