Privacy Policy

Introduction

This Privacy Policy sets out how the **Prince of Peace Lutheran College** manages personal information provided to, or collected by it.

The College is bound by the Australian Privacy Principles contained in the Commonwealth Privacy Act.

The College may, from time to time, review and update this Privacy Policy 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.

1. Personal Information collected and how it is collected

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

- pupils and parents and/or guardians ('Parents') before, during and after the course of a pupil's enrolment at the College.
- job applicants, staff members, volunteers and contractors.
- other people who come into contact with the College.

1.1 Personal Information provided by individuals:

The College 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, emails and telephone calls. On occasions people other than Parents and pupils provide personal information.

1.2 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 College.

.

1.3 Exception in relation to employee records:

Under the Privacy Act, the Australian Privacy Principles do not apply to an employee record. As a result, this 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.

2. How Prince of Peace Lutheran College intends to use the personal information provided

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 reasonably expected by you, or to which you have consented.

2.1 Pupils and Parents:

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

The purposes for which the College 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 of the College.
- looking after pupils' educational, social and medical wellbeing.
- seeking donations and marketing for the College.
- 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 pupil or parent, if the information requested is not provided, the College may not be able to enrol or continue the enrolment of the pupil or permit the pupil to take part in a particular activity.

2.2 Job applicants, staff members and contractors:

In relation to personal information of job applicants, staff members and contractors, the College'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 College 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 donations and marketing for the College.
- to satisfy the College's legal obligations, for example, in relation to child protection legislation.

2.3 Volunteers:

The College also obtains personal information about volunteers who assist the College in its functions or conduct associated activities, such as Parent and Friends Association, including its sub groups.

2.4 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, for example, the College's Foundation or College Parents & Friends.

Parents, staff, contractors and other members of the wider College community may from time to time receive fundraising information. College publications, like newsletters and magazines, which include personal information, may be used for marketing purposes.

3. Disclosure of personal information

The College may disclose personal information, including sensitive information, held about an individual to:

- government departments.
- medical practitioners.
- people providing services to the College, including specialist visiting teachers, counsellors and sports coaches.
- recipients of College publications, such as newsletters and magazines;
- parents.
- anyone you authorise the College to disclose information to.
- anyone to whom we are required to disclose the information to by law.

3.1 Sending information overseas:

The College 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 College exchange. 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).
- otherwise complying with the Australian Privacy Principles or other applicable privacy legislation.

4. The treatment of 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 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 the sensitive information is allowed by law.

5. Management and security of personal information

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

The College has in place steps to protect the personal information the College 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.

5.1 Access and correction of personal information

Under the Commonwealth Privacy Act, an individual has the right to obtain access to any personal information which the College holds about them and to advise the College of any perceived inaccuracy. Students can obtain and correct information through their parents.

To make a request to access or update any personal information the College holds about you or your child, please contact the College Privacy Officer in writing. 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. If we cannot provide you with access to that information, we will provide you with written notice explaining the reasons for refusal.

6. Consent and rights of access to the personal information of pupils

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 pupil to the pupil's parents. The College 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.

As mentioned above, parents may seek access to personal information held by the College about them or their child by contacting the College Privacy Officer. 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 College's duty of care to the pupil.

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

7. Response to Data Breaches

Response plan

In the event of a Data Breach, the College will adhere to the four phase process set out below (as described in the Office of the Australian Information Commissioner's (OAIC) Notifiable Data Breaches scheme: Resources for agencies and organisations. Appropriate records and any evidence will be kept of the Data Breach and the response. Legal advice should also be sought if necessary.

Phase 1. Confirm, contain and keep records of the Data Breach and do a preliminary assessment

1. The College personnel who become aware of the Data Breach or suspects a Data Breach has occurred must immediately notify the College Privacy Officer. That person must take any immediately available steps to identify and contain the Data Breach and consider if there are any other steps that can be taken immediately to mitigate or remediate the harm any individual could suffer from the Data Breach.
2. In containing the Data Breach, evidence should be preserved that may be valuable in determining its cause.
3. The College Privacy Officer must make a preliminary assessment of the risk level of the Data Breach. The following table sets out examples of the different risk levels.

Risk Level	Description
High	Large sets of personal information or highly sensitive personal information (such as health information) have been leaked externally.
Medium	Loss of some personal information records and the records do not contain sensitive information. Low Risk Data Breach, but there is an indication of a systemic problem in processes or procedures.
Low	A few names and school email addresses accidentally disclosed to trusted third party (e.g. where email accidentally sent to wrong person). Near miss or potential event occurred. No identified loss, misuse or interference of personal information.

4. Where a **High Risk** incident is identified, the College Privacy Officer must consider if any of the affected individuals should be notified immediately where serious harm is likely.
5. the College Privacy Officer must escalate High Risk and Medium Risk Data Breaches to the response team (whose details are set out at the end of this policy).
6. If there could be media or stakeholder attention as a result of the Data Breach, it must be escalated to the response team.

Phase 2. Assess the Data Breach and evaluate the risks associated with the Data Breach including if serious harm is likely

1. The response team is to take any further steps (i.e. those not identified in Phase 1) available to contain the Data Breach and mitigate or remediate harm to affected individuals.
2. The response team is to work to evaluate the risks associated with the Data Breach, including by:
    a. identifying the type of personal information involved in the Data Breach;
    b. identifying the date, time, duration, and location of the Data Breach;
    c. establishing who could have access to the personal information;
    d. establishing the number of individuals affected; and
    e. establishing who the affected, or possibly affected, individuals are.
3. The response team must then assess whether the Data Breach is likely to cause serious harm to any individual whose information is affected by the Data Breach, in which case it should be treated as an eligible Data Breach (EDB).
4. The response team should also consider whether any of the limited exceptions apply to the Data Breach if it is otherwise an EDB.

5. All reasonable steps must be taken to ensure that the assessment is completed as soon as possible and in any event within 30 days after they suspect there has been a Data Breach.

Phase 3. Consider Data Breach notifications

6. The response team must determine whether to notify relevant stakeholders of the Data Breach, including affected individuals, parents and the OAIC even if it is not strictly an EDB.
7. As soon as the response team knows that an EDB has occurred or is aware that there are reasonable grounds to believe that there has been an EDB, they must prepare a statement with the prescribed information and give a copy of the statement to the Information Commissioner.
8. After completing the statement, unless it is not practicable, the response team must also take such reasonable steps to notify the contents of the statement to affected individuals or those who are at risk from the EDB.
9. If it is not practicable to notify some or all of these individuals, the response team must publish the statement on their website, and take reasonable steps to otherwise publicise the contents of the statement to those individuals.

Phase 4. Take action to prevent future Data Breaches

10. The response team must complete any steps in Phase 2 above that were not completed because of the delay this would have caused in proceeding to Phase 3.
11. The College Privacy Officer must enter details of the Data Breach and response taken into a Data Breach log. The College Privacy Officer must, every year, review the Data Breach log to identify any reoccurring Data Breaches.
12. The College Privacy Officer must conduct a post-breach review to assess the effectiveness of the School's response to the Data Breach and the effectiveness of the Data Breach Response Protocol.
13. The College Privacy Officer must, if necessary, make appropriate changes to policies, procedures and staff training practices, including updating this Data Breach Response Protocol.
14. The College Privacy Officer must, if appropriate, develop a prevention plan to address any weaknesses in data handling that contributed to the Data Breach and conduct an audit to ensure the plan is implemented.

Enquiries

If you would like further information about the way the College manages the personal information it holds, or wish to complain that you believe that the College has breached the Australian Privacy Principles, please contact the College Privacy Officer. Note that all requests for information held under privacy legislation must be in writing.

All enquiries regarding privacy matters or access to information should be forwarded to the College's Privacy Officer at:

College Privacy Officer
Prince of Peace Lutheran College
20 Rogers Parade West
EVERTON HILLS QLD 4053 or email: privacyofficer@princeofpeace.qld.edu.au

Complaints

An individual whose personal information is/has been held by the College, may lodge a complaint in writing to the College Privacy Officer about an act or practice of Prince of Peace which the individual believes to be inappropriate or unlawful.

The Privacy Officer will investigate the complaint and report to the Head of College. A decision will be made concerning the complaint and the complainant will be advised in writing of the result of the investigation.

Information collected by the College with regard to a person's employment is exempt.