SP 1.3: PROCEDURES FOR PRIVACY

1.0 Management of information

1.1 Collection of Information

1.1.1 Purpose of collection

- Information is collected for the primary purpose of providing every student with the opportunity to achieve their educational potential and for other directly related purposes including but not limited to:
- implementing action that aid in meeting student educational and support needs
- communicating with parents and carers
- maintaining the good order and management of the School
- ensuring the safety and welfare of students, staff and others involved with the school's operation
- conducting lawful research and compiling statistics relating to the education, health, welfare and wellbeing of students and student performance
- assessing and evaluating the effectiveness of School decisions and their impact on student educational outcomes
- operational and administrative purposes
- determining whether students are meeting compulsory school requirements

1.1.2 Method of collection

1.1.2.1 Personal information provided directly:

The School will generally collect personal information held about an individual by way of forms filled out by parents or pupils, emails, face-to-face meetings and interviews, and telephone calls. On occasions, people other than parents and pupils provide personal information.

1.1.2.2 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.

1.1.2.3 Exception in relation to employee records:

Under the Privacy Act and the Health Records Act the Australian Privacy Principles and Health Privacy Principles do not apply to the School's treatment of 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. The School handles staff health records in accordance with the Health Privacy Principles in the Health Records Act.

1.1.2.4 Collection of solicited personal information

The School must not collect personal information unless the information is reasonably necessary for, or directly related to, one or more of its functions or activities. Subject to a number of exceptions, Schools can only collect "sensitive information" if the individual consents to the collection.

1.1.2.5 Dealing with unsolicited information

If the School receives personal information that it did not solicit, it must decide whether or not it could have collected the information under APP 3. If not, the School must, as soon as practical, destroy the information or ensure it is de-identified.

1.2 Use of personal information

The School will use personal information it collects for the primary purpose of database collection, and for such other secondary purposes as defined below.

1.2.1 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 pupils enrolled at the School, exercise its duty of care, and perform necessary associated administrative activities, which will enable pupils to take part in all the activities of the School. 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 about 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 and school management purposes;
- looking after pupils' educational, social, spiritual and medical wellbeing;
- to satisfy the School's legal obligations and allow the School to discharge its duty of care;
- to maintain accurate administration records for reporting to government authorities.

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 maintain its educational function towards a child, and as a result may not be able to enrol or continue the enrolment of the pupil.

1.2.2 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.

1.2.3 Volunteers

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

1.3 Disclosure of personal information

All records on students kept by the School are maintained on a student file. Information held on student files may be released only in accordance with the provisions of the Information Privacy Act 2002.

The presumption of confidentiality is overridden in circumstances where there is a legal or departmental requirement to disclose information or where one or more individuals may experience serious harm if someone with the power to act is not informed.

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, medical officers and sports coaches;
- assessment and educational authorities, including the Australian Curriculum, Assessment and Reporting Authority;
- people providing administrative and financial services to the School'
- recipients of School publications, newsletters, magazines or electronic media;
- students parents or guardians;
- anyone the individual authorises the School to disclose information to; and
- anyone to whom the School is required to disclose the information by law, including child protection laws.

1.3.1 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 Australian Privacy Principles or other applicable privacy legislation.

The School may use online or 'cloud' service providers to store personal information and to provide services to the School 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 a cloud service provider's servers which may be situated outside Australia.

1.3.2 Cloud Service Provider

The School utilises Sentral, a School Management System, which facilitates the storage and use of a range of information pertaining to students, staff and school families. This application is hosted locally on the school's physical servers but has an online external access port for offsite use. Sentral is backed up regularly and securely to a cloud service hosted and managed by the Sentral software provider.

1.3.3 Cross-border disclosure of personal information

Where the School discloses personal information to an overseas recipient (such as a cloud service provider), it will take reasonable steps to ensure that the overseas recipient does not breach the APPs. The School will be legally accountable if the overseas recipient mishandles the personal information, unless the School has the individual's consent to the overseas disclosure, or the School satisfies itself that the overseas recipient is subject to the laws of a country, or a binding scheme, that it reasonably believes to be substantially similar to the protections provided by the 13 APPs and the individual can access a mechanism to enforce those protections.

1.3.4 Direct marketing

The School must not use or disclose personal information it has collected from an individual for the purpose of direct marketing unless it has the individual's consent, or if it is impractical to obtain consent for each direct marketing communication, the School provides the individual with the ability to "opt out" of receiving future direct marketing communications.

Sensitive information cannot be used for direct marketing purposes without an individual's consent.

2.0 Computer, internet and digital technology

Personal information may be collected, used, disclosed, stored and transferred overseas through the use of email and internet facilities.

In the course of carrying out duties on behalf of the School, volunteers, contractors, teachers and all other support staff may have access to or handle personal information relating to others, including students, colleagues, contractors, parents and suppliers. Email should not be used to disclose personal information of another except in accordance with the School's Privacy Policy or with proper authorisation.

The Privacy Act requires both the School and the user of the computer, internet or other information technology to take reasonable steps to protect the personal information that is held, from misuse and unauthorised access.

The school stresses, therefore, that users take responsibility for the security of personal computers and not allow them to be used by an unauthorised party, which specifically includes anyone who is not an employee of the School.

Users will be assigned a log-in code and a password to use the School's electronic communications facilities. These details are not to be disclosed to anyone else. In order to keep these details secure, passwords must be changed regularly and log-in codes and passwords are not to be kept in writing close to the working area.

Teachers are to ensure that students cannot gain unauthorised access to personal information and confidential information within the School.

In order to comply with the School's obligations under the Privacy Act, staff are encouraged to use the blind copy option when sending emails to multiple recipients where disclosure of those persons' email addresses will impinge upon their privacy.

In addition to the above, school employees and volunteers should familiarise themselves with the Australian Privacy Principles (**'APPs'**), P4.4: Policy for Computer, Internet and Digital Technologies and ensure that their use of email does not breach the Privacy Act or the NPPs. Anyone who requires more information on the Privacy Act and how to comply, may contact the School Principal.

3.0 Management and security of personal information

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. Information collected, used and/or disclosed is to be accurate, up-to-date, complete and relevant.

Where the School no longer needs the personal information it must be destroyed.

4.0 Privacy Program

In accordance with the School's Privacy Program, the School will regularly conduct the following:

- review and test the strength of its security measures which protect personal information
- establish any compliance gaps by carrying out a *Personal Information Management Audit*
- develop procedures to ensure the School's NDP obligations will be met if an eligible data breach occurs
- communicate the NDB procedures to member of the school community; and
- train all staff with respect to their privacy obligations and the NDB requirements.

5.0 Privacy breach

In the event of a Privacy Breach, the following four phase process provides details of the School's required response. Phases 1 – 3 should occur in quick succession and may occur simultaneously. See Appendix 1 for full details.

- Phase 1. Contain the Privacy Breach and do a preliminary assessment
- Phase 2. Evaluate the risks associated with the Privacy Breach
- Phase 3. Consider Privacy Breach notifications
- Phase 4. Take action to prevent future Privacy Breaches

5.1 Notifiable Data Breach

A data breach occurs where personal information held by an agency or organisation is lost or subjected to unauthorised access, modification, disclosure, or other misuse or interference.

A *Notifiable Data Breach (NDB)* is defined as a data breach that is likely to result in serious harm to any of the individuals to whom the information relates.

Where an eligible data breach is believed to have occurred, the School will:

- Carry out a risk assessment
- Prepare a statement of prescribed information regarding the eligible data breach believed to have occurred
- Submit this statement to the Office of the Australian Information Commissioner (OAIC); and contact
- All affected individuals directly or indirectly by publishing information about the eligible data breach on publicly accessible forums.

5.2 Risk assessment of a data breach

If the School suspects that an eligible data breach has occurred, the School must conduct a risk assessment which involves:

- Promptly assessing whether there are reasonable grounds to believe that the relevant circumstances amount to an eligible data breach; and
- Taking all reasonable steps to ensure that the assessment is completed within 30 days after becoming aware of the breach.

If the risk assessment reveals that an eligible data breach has occurred, the School must then follow the notification requirements under the Act and notify both the OAIC and if practicable, the individual/s affected.

5.3 Notifying the OAIC

Where the School has reasonable grounds to believe that there has been an eligible data breach, the School must:

- Prepare a Statement in the prescribed format; and
- Give a copy of the Statement to the OAIC as soon as practicable after the School becomes aware of the eligible data breach. The Statement must set out the School's identity and contact details, a description of the eligible data breach, the kind of information concerned, and recommendations about the steps that individuals should take in response to the eligible data breach.

5.4 Notifying the Individual

As soon as practicable after notifying the OAIC, the School must take such steps as are reasonable in the circumstances to:

- Notify each of the individuals to whom the relevant information relates; or
- Notify each of the individuals who are *at risk* from the eligible data breach.

If neither of the above options apply, the School must:

- Publish a statement on the School website; and
- Take reasonable steps to publicise the contents of the Statement it prepared for the OAIC.

6.0 Access and correction to personal information

Under the Commonwealth Privacy Act, an individual has the right to seek and obtain access to any personal information, which the School holds about them and to advise the Principal or 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.

The School will take reasonable steps to correct any personal information that is inaccurate, out of date, incomplete, irrelevant or misleading. Where the individual has requested the School to do so, notification will be given to another organisation of any corrections made to any information disclosed to the organisation.

6.1 Student Information and Parent Access

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. Although the Privacy Act does not differentiate between adults and children, 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. To request access to any information the School holds about a child, the parent should contact the School's Principal in writing. If the information sought is extensive, the School may levy a likely cost in advance.

The School may, at its discretion, on the request of a pupil, grant that pupil access to information held by the School about him/her, or allow a pupil to give or withhold consent to the use of his/her personal information, independently of his/her parents. This would normally be done only when the maturity of the pupil and/or the pupil's personal circumstances so warrant.

Where a student requests that personal information, particularly sensitive information, not be disclosed to parents will be dealt with on a case by case basis.

6.2 Withheld Access to Information

There will be occasions where access to information 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.

7.0 Procedure Review Statement

These procedures are to be reviewed every two years.

8.0 References and Related Documents

Privacy and Personal Information Protection Act 1998
Freedom of Information (FOI) Act, 1989
Children and Young Persons (Care and Protection) Act 1998
Public Finance & Audit Act 1983
P1.2 Complaints and Appeals
SP1.2 Complaints and Appeals
P1.3 Policy for Privacy
P4.3 Communication Policy
P4.4 Information and Communication Technologies
Australian Privacy Principles

Appendix 1
Response to Privacy Breach - Four Phase Process

Phase 1. Contain the Privacy Breach and do a preliminary assessment

1. The School personnel who becomes aware of the Privacy Breach must immediately notify the Privacy Officer. This notification should include (if known at this stage) the time and date the suspected Privacy Breach was discovered, the type of personal information involved, the cause and extent of the Privacy Breach, and who may be affected by the Privacy Breach.
2. The Privacy Officer must take any immediately available steps to contain the Privacy Breach (e.g. contact the IT department, if practicable, to shut down relevant systems or remove access to the systems).
3. In containing the Privacy Breach, evidence should be preserved that may be valuable in determining the cause of the Privacy Breach. This is particularly relevant if there is a Privacy Breach involving information security.
4. The Privacy Officer must consider if there are any other steps that can be taken immediately to mitigate the harm an individual may suffer from the Privacy Breach.
5. The Privacy Officer must make a preliminary assessment of the risk level of the Privacy Breach. This will involve an analysis of the risks involved. The following table sets out examples of the different risk levels.

Risk Level Description

1. In the event that the Privacy Officer receives multiple reports of Privacy Breaches of different datasets, this may be part of a related incident. The Privacy Officer must consider upgrading the risk level if this situation arises.

2. Where a High Risk incident is identified, the Privacy Officer must consider if the affected individuals should be notified immediately to mitigate the risk of serious harm to the individuals.

3. The Privacy Officer must escalate High Risk and Medium Risk Privacy Breaches to the response team.

4. If the Privacy Officer believes a Low Risk Privacy Breach has occurred, he or she may determine that the response team does not need to be convened. In this case, he or she must undertake Phases 2 and 3 below.

5. If there could be media or stakeholder attention as a result of the Privacy Breach, it must be escalated to the response team.

6. If appropriate, the response team should pre-empt media interest by developing a communications or media response and strategy that manages public expectations.

Phase 2. Evaluate the risks associated with the Privacy Breach

1. The response team is to take any further steps (i.e. those not identified in Phase 1) available to contain the Privacy Breach and mitigate harm to affected individuals.

2. The response team is to work to evaluate the risks associated with the Privacy Breach by:
    a) identifying the type of personal information involved in the Privacy Breach;
    b) identifying the date, time, duration, and location of the Privacy Breach;
    c) establishing the extent of the Privacy Breach (number of individuals affected);
    d) establishing who the affected, or possibly affected, individuals are;
    e) identifying what is the risk of harm to the individual/s and the extent of the
    f) likely harm (eg what was the nature of the personal information involved);

g) establishing what the likely reoccurrence of the Privacy Breach is;
h) considering whether the Privacy Breach indicates a systemic problem with
i) practices or procedures;
j) assessing the risk of harm to the School and [AIS/CEC]; and
k) establishing the likely cause of the Privacy Breach.

3. The response team should assess priorities and risks based on what is known.

4. The response team does not need to consider a particular matter above if this will cause significant delay in proceeding to Phase 3.

5. The response team should regularly update each other and other relevant stakeholders regarding incident status.

Phase 3. Consider Privacy Breach notifications

1. Where appropriate, having regard to the seriousness of the Privacy Breach (based on the evaluation above), the response team must determine whether to notify the following stakeholders of the Privacy Breach:

    a) affected individuals;
    b) parents;
    c) the OAIC; and/or
    d) other stakeholders (e.g. if information which has been modified without
    e) authorisation is disclosed to another entity, that entity may need to be notified).

2. In general, if a Privacy Breach creates a real risk of serious harm to the individual, the affected individuals (and their parents if the affected individuals are pupils) and the OAIC should be notified.

3. The response team will facilitate ongoing discussion with the OAIC as required.

Phase 4. Take action to prevent future Privacy Breaches

1. 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. The cause of the Privacy Breach must be fully investigated

2. The Privacy Officer must enter details of the Privacy Breach and response taken into a Privacy Breach log. The Privacy Officer must, every year, review the Privacy Breach log to identify any reoccurring Privacy Breaches.

3. The Privacy Officer must conduct a post-breach review to assess the effectiveness of the School's response to the Privacy Breach and the effectiveness of the Privacy Breach Response Protocol.

4. The Privacy Officer must, if necessary, make appropriate changes to policies, procedures and staff training practices, including updating this Privacy Breach Response Protocol.

5. The Privacy Officer must, if appropriate, develop a prevention plan to address any weaknesses in data handling that contributed to the Privacy Breach and conduct an audit to ensure the plan is implemented