FSAC Ltd

Board Policy No. 3
Compliance Management

Privacy Procedure No.3.2

2014

Authorisation Originator	Board Approval Date
Print Name Chairman of the Board	Signature Chairman of the Board

Version Control	
Current Version Number	# 2.
Effective Date	30/06/2014
Review Date	30/06/2015

1. POLICY STATEMENT

Board Policy No 3. – Compliance Management

2. PROCEDURE STATEMENT

The Board is committed to managing personal and sensitive information and the protection of the privacy of students, families, staff, volunteers and other College stakeholders in an appropriate and respectful manner.

2.1. Scope

This procedure applies to students, parents, Board members, employees and volunteers.

2.2. Principles

The Colleges collect, hold, use and discloses personal information so that they can exercise their function and activities and fulfil relevant duties and obligations.

That may include (but is not limited to):

(a) informing Parents about the Student's education;
(b) College administrative purposes, including for the provision of such services to the School;
(c) supporting a Student's educational, social and medical wellbeing;
(d) seeking donations and/or marketing for the Colleges; and
(e) satisfying the legal obligations of the Colleges.

The Colleges collect and hold personal information, sensitive information and health information about Students, Parents and Employees.

The Colleges generally deal with personal and sensitive information regarding:

(f) Students and Parents relating to the enrolment of the Student at the Colleges;
(g) job applicants, staff members, volunteers and contractors; and
(h) persons who are involved with the Colleges.

The Colleges collect personal information about individuals to satisfy legal obligations and to fulfil their educational purpose. If the Colleges request information to be provided and the request is not complied with, the Colleges may be unable to enrol a prospective Student or continue enrolment of a current Student.

2.3. Affiliated Authorities

- *Privacy Act (Cwlth) 1988 (as amended 2012).*
- Australian Privacy Principles (APPs) (refer Appendix 1.)

3. DEFINITIONS

Employee means all employees employed by the School, including applicants and prospective Employees.

Employee Record means a record as defined in the Act.

Parent is the parent / guardian / carer of a Student.

Student means prospective, current or past student of the School.

Personal information is information or an opinion, whether true or not, and whether recorded in material form or not, about an identified individual or an individual whose identity is reasonably apparent, or can be determined, from the relevant information or opinion.

Sensitive information is a type of personal information. It includes information or opinion about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual preference or practice, or criminal record. Sensitive information also includes biometric information that is used for the purpose of automated biometric verification, biometric identification or biometric templates.

Health information is a subset of sensitive information. It is information or an opinion about the health or disability of an individual and information collected to provide, or in providing a health service.

Health service includes an activity performed to assess, record, maintain or improve an individual's health, to diagnose an illness or disability, to treat an individual, or the dispensing on prescription of a drug or medicinal preparation by a pharmacist.

4. COLLECTION

4.1. Personal Information

The Colleges collect personal information about an individual by way of forms, face-to-face meetings, interviews and telephone calls. Other individuals may provide personal information about a person in dealings with the Colleges.

The Colleges may collect personal information about an individual from a third party, for example, a medical practitioner providing a report.

Collection of personal information from a third party will be undertaken where it is reasonably necessary to do so. Any personal information that is unsolicited will be dealt with in accordance with the APPs.

4.2. Sensitive Information

Sensitive information will be collected by the Colleges where it is reasonably necessary for one or more of the Colleges' functions or activities. It will only be collected with consent, unless one of the exceptions under the APPs applies.

4.3. Employee Records

Under the Act, the APPs do not apply to Employee records. This means that the Act does not apply to how the Colleges deal with an Employee record that concerns current and former Employees of the Colleges.

5. USE AND DISCLOSURE

The Colleges will only use and disclose personal information for the primary purpose of collection or as otherwise specified in this Privacy Procedure.

The Colleges may disclose personal information to the Corporation of Synod of the Diocese of Brisbane for administrative and management purposes including insurance, child protection and professional standards.

Personal information will only be used for a secondary purpose if consent has been obtained, where it is reasonably expected or if such use or disclosure falls within a permitted exception.

Sensitive information will be used and disclosed for the primary purpose of collection, unless the Colleges are advised otherwise, or the use or disclosure is required / permitted by law.

6. QUALITY OF INFORMATION AND SECURITY

The Colleges endeavour to ensure that the personal information they hold is accurate, complete and up to date.

The Colleges will take all reasonable steps to:

(i) protect personal information from misuse, interference, loss, unauthorised access, modification or unauthorised disclosure; and

(j) destroy or de-indentify information that is no longer needed.

7. ACCESS TO PERSONAL INFORMATION

Access to records of personal information that the Colleges hold or concerns about the accuracy of information held by the Colleges should be directed to the Head of College or their delegate.

Under the Act, an individual has the right to obtain access to personal information which the Colleges holds about them; there are exceptions to this, for example, where access may impact the privacy of others or pose as a threat to the individual.

To make a request to access personal information the Colleges requires a request in writing. The Colleges will respond to this request within a reasonable 14 days from the receipt of the application. Where it is reasonable, the Colleges will provide access in the manner requested. The Colleges may charge a fee to provide access to the personal information, however, will not charge for the request for access.

If a request for access is refused the Colleges will provide written reason on why the request was refused; details on how to make a complaint will also be included in this response.

8. JOB APPLICANTS AND CONTRACTORS

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

- Administering the individual's employment or contract;
- For insurance purposes
- Seeking funds and marketing for the Colleges, and
- To satisfy the Colleges' legal, compliance and due diligence obligations.

9. VOLUNTEERS

The Colleges obtain personal information about volunteers who assist the Colleges in their functions or who conduct associated activities. This information enables the Colleges and volunteers to work together.

10. MARKETING AND FUNDRAISING

The Colleges engage in marketing and fundraising as a means to promote future growth and sustain and improve the educational environment for Students.

Personal information collected may be used to make a marketing or fundraising appeal. The Colleges will abide by any direction from an individual not to disclose personal information to third parties for marketing purposes.
The Colleges also allows individuals to "opt out" through selection on the enrolment agreement.

11. STUDENT PHOTOS AND VIDEOS

The Information Privacy Act 1988 covers the collection and use of personal Information. Personal Information is information which identifies a person. A

photograph or video image of a student is personal information and must be treated in accordance with the above.

Enrolment Agreement
Clause 2 b) of the College Enrolment Agreement provides for a general permission for the student's photograph being used in College publications. This clause in effect is a condition of enrolment unless specifically excluded.

General use of Student images and videos
The Colleges will generally not obtain permission (subject to the reference to the Enrolment Agreement above) for the use of student images for:

- Included in College magazines and/or year books
- College newsletters or electronic media
- Photos taken by an authorised member of the press, eg when a local politician visits the Colleges and brings a press photographer along

These situations are generally for the purpose of praising or promoting the efforts of the students or the Colleges and are reasonable expected use of the student images as identified when enrolling at the Colleges.

Use of Student images for Direct Marketing Purposes
Situations where a photo or video is to be used for direct marketing or the photo or video is to be placed in the public domain, such as the print or electronic media, specific permission will be obtained from the parent/guardian.

Avoiding Unauthorised Use of Student Images
Parents/Guardians should notify the Head of College immediately if any circumstances arise that would prevent the Colleges from using their child's photo or video images being used as outlined above.

12. STAFF PRIVACY

The Colleges keep a personal file for each employee. Information kept in these files includes:

- Personal information as provide by the employee
- Personal information provided by another person that relates to the employee
- Wages information; accident/incident reports; memos to/from the employee; leave information and other payroll related information
- Information that relates to the performance and development of the employee

The primary purpose of recording personal information relating to employees is to facilitate correspondence with the employee on matters related to their employment with the Colleges. Only senior staff members or other staff working under the direction of a senior staff member will have access to the information contained on an employee's personal file. Except where legally permitted or where consent has been obtained, the Colleges will not disclose personal information about an employee to a third party. An employee may request to see information that has recorded about them. Such as request should be made to the Manager HR & Compliance.

13. 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 school exchange.

14. UPDATING PERSONAL INFORMATION

The Colleges endeavor to ensure that the personal information they hold is correct, complete and up-to-date. A person may seek to update their personal information held by the Colleges by contacting the Head of College at any time.

15. ACCESS AND CORRECTION OF PERSONAL INFORMATION

An individual has the right to obtain access to any personal information the Colleges hold about them and to advise the Colleges of any perceived inaccuracies. There are some exceptions to this right set out in the legislation. Students will generally have access to their personal information through their parents, but older students may seek access themselves.

16. COMPLAINTS

If an individual believes that the Colleges have breached the APPs a complaint can be made to the College.

All complaints should be in writing and directed to the Manager HR & Compliance. The Colleges will investigate complaints in a timely manner and respond in writing.

If an individual is not satisfied with the Colleges' response, a complaint can be lodged with the Office of the Australian Information Commissioner on the following website http://www.oaic.gov.au/privacy/making-a-privacy-complaint.

17. PROCEDURE ADMINISTRATION

In accordance with procedure development and review protocol this procedure will be recorded as an authorised procedure approved by the Heads of College, at its meeting of the date shown on the front of this procedure document.

The procedure will be reviewed twelve (12) months from the date of the approval shown herein.

Notwithstanding the schedule review, should any circumstance change significantly before the twelve (12) month review period, the policy will be immediately reviewed in order to maintain appropriate accuracy, relevance and authority.

Privacy Act (Cth) 1988 (as amended 2012)
Australian Privacy Principles (APPs)

APP 1 – Open and transparent management of personal information
This principle requires organisations to have ongoing practices and policies in place to ensure that they manage personal information in an open and transparent way. It also introduces a positive obligation for organisations to implement practices, procedures and systems that will ensure compliance with the APPs and any registered APP codes, including a system in place to deal with complaints from individuals concerning compliance.

APP 2 – Anonymity and pseudonymity
This principle sets out a requirement that an organisation provide individuals with the option of dealing with it using a pseudonym. This obligation is in addition to the existing requirement that organisations provide individuals with the option of dealing with them anonymously. Both requirements are subject to certain limited exceptions, including where it is impracticable for the organisation to deal with an individual who has not identified themselves, or where the law or a court/tribunal order requires or authorises the organisation to deal with individuals who have identified themselves.

APP 3 – Collection of solicited personal information
This principle outlines when and how an organisation may collect personal and sensitive information that it solicits from an individual or another entity. An organisation must not collect personal information (other than sensitive information) unless the information is reasonably necessary for one or more of the organisation's functions or activities. It clarifies that, unless an exception applies, sensitive information must only be collected with an individual's consent if the collection is also reasonably necessary for one or more of the organisation's functions or activities. Sensitive information can be collected without consent if a "general permitted situation" or "general health situation" exists. An organisation must only collect personal information from the individual, unless it is unreasonable or impracticable to do so.

APP 4 – Dealing with unsolicited personal information
This principle creates obligations in relation to the receipt of personal information which is not solicited. Where an organisation receives unsolicited personal information, it must determine whether it would have been permitted to collect the information under APP 3. If an organisation finds that is it not permitted to hold the personal information then they must destroy or de-identify the information, unless it is not lawful or reasonable to do so.

APP 5 – Notification of the collection of personal information
This principle requires that an organisation notify an individual when they collect personal information. This generally addressed by issuing a standard collection notice. However, an organisation will have to provide further notice when:

(a) they receive information about an individual from a third party; and
(b) they collect information that is required or authorised by Australian law, court, or tribunal order.

APP 6 – Use and disclosure of personal information
This principle provides that an organisation must only hold and use information for a primary purpose, and must not use and disclose for a secondary purpose unless an exception applies. The exceptions are:

(a) the individual has consented to the use or disclosure of the information;
(b) the individual would reasonably expect the school to disclose the information for the secondary purpose;
(c) use or disclosure of the information is required or authorised by Australian law, court, or tribunal order;
(d) a permitted general situation exists;

(e) a permitted health situation exists; or
(f) the organisation reasonably believes that the use or disclosure of information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.

APP 7 – Direct marketing
Generally, organisations may only use or disclose personal information for direct marketing purposes where the individual has either consented to their personal information being used for direct marketing, or has a reasonable expectation that their personal information will be used for this purpose, and conditions relating to opt-out mechanisms are met. The organisation must provide an "opt-out" option (this would ordinarily be provided in the standard collection notice).

APP 8 – Cross-border disclosures
This principle introduces an accountability approach to organisations' cross-border disclosures of personal information.

APP 9 – Adoption, use or disclosure of government related identifiers
This principle prohibits an organisation from adopting, using or disclosing a government related identifier unless an exception applies.

APP 10 – Quality of personal information
Under this principle an organisation must take reasonable steps to ensure the personal information it collects is accurate, up-to-date and complete.For uses and disclosures, the personal information must be relevant, as well as, accurate, up-to-date and complete, having regard to the purpose of the use or disclosure.

APP 11 – Security of personal information
This principle requires an organisation to take reasonable steps to protect the personal information it holds from interference, in addition to misuse and loss, and unauthorised access, modification and disclosure. Under this principle there are two exceptions to this requirement:

- the personal information is contained in a Commonwealth record, or
- the organisation is required by or under an Australian law or a court/tribunal order to retain the information.

APP 12 – Access to personal information
The APPs separate the access and correction requirements into two separate principles. This principle requires an organisation to give an individual access to the personal information that it holds about that individual, unless an exception applies. There is a new requirement for organisations to respond to requests for access within a reasonable period. In addition, organisations must give access in the manner requested by the individual if it is reasonable to do so. If an organisation decides not to give an individual access, it must generally provide written reasons for the refusal and the mechanisms available to complain about the refusal.

APP 13 – Correction of personal information
This principle requires an organisation to take reasonable steps to correct personal information to ensure that, having regard to a purpose for which it is held, it is accurate, up-to-date, complete, relevant and not misleading, if either:

- the organisation is satisfied that it needs to be corrected, or
- an individual requests that their personal information be corrected.

An organisation must also respond to a correction request or a request to associate a statement by the individual within a reasonable period after the request is made, and must not charge the individual for making the request, for correcting the personal information, or for associating the statement with the personal information. When refusing an individual's correction request, an organisation must generally

provide the individual with written reasons for the refusal and notify them of available complaint mechanisms.