Privacy Policy

Preamble

This policy outlines how Mount St Benedict College uses and manages personal information provided to, or collected by it, about students, parents and guardians before and during the course of a pupil's enrolment at the College, job applicants, staff members, volunteers, contractors and others including past students, visitors and others than come into contact with the College. The College is bound by the Australian Privacy Principles (APPs) contained in the Commonwealth Privacy Act. In relation to health records, the College is also bound by the New South Wales Privacy Principles which are contained in the Health Records and Information Privacy Act 2002 (Health Records Act).

Principles

The College will comply with the Australian Privacy Principles (APPs) and any other relevant laws relating to the collection, storage, use, access, collation and disclosure of personal information. Information that this policy refers to includes personal, sensitive and health information.

The primary purpose of collecting this information is to enable the College to provide appropriate educational opportunities for its students, to satisfy legal obligations and to facilitate the College's duty of care. Enrolment of a student is contingent upon the receipt of such information.

This policy applies to all records, including electronic and digital records, held by the College, including voice mails and other sound encodings.

The College Privacy Policy is to be accessible and will be distributed to all current staff and relevant personnel.

Collection of personal information

The College will only collect information that is necessary.

The College may collect and hold personal information, including sensitive information about (though not limited to):
Students and parents and/or guardians before, during and after the course of a student's enrolment at Mount St Benedict College;

- job applicants, staff members, volunteers and contractors; and
- past students, visitors and other people who come into contact with the College.

A Privacy Collection Notice will be issued whenever the College collects personal information.

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

The kinds of personal information the College collects and how it is collected is largely dependent upon whose information is being collected and why we are collecting it, however in general terms the College may collect:

- Personal Information – including names, addresses and other contact details; dates of birth; next of kin details; financial information, photographic images and attendance records.
- Sensitive Information – including religious beliefs, government identifiers, nationality, country of birth, languages spoken at home, professional membership, family court orders and criminal records.
- Health Information – including medical records, disabilities, immunisation details, individual health care plans, counseling reports, nutrition and dietary requirements

Where is it reasonable and practical to do so, the College will collect personal information directly from the individual.

Where possible the College has attempted to standardize the collection of personal information by using specifically designed form (e.g. an Enrolment Form). However, given the nature of College operations, we often receive personal

information by email, letters, notes, over the telephone, in face to face meetings, through financial transactions and through surveillance activities such as the use of CCTW security cameras or email monitoring.

The College may also collect personal information from other people (e.g. a reference or report from medical professional) or independent sources (e.g. a telephone directory), however we will only do so where it is not reasonable and practicable to collect the information directly.

Sometimes the College may be provided with personal information without having sought it through our normal means of collection. This is referred to as "unsolicited information". Where unsolicited information is collected, the College will only hold, use and/or disclose that information if we could otherwise do so had we collected it by normal means. If that unsolicited information could not have been collected by normal means then the information will be destroyed, permanently deleted or de-identified as appropriate.

Use and disclosure of personal information

The College only uses personal information that is reasonably necessary for one or more of our functions or activities (the primary purpose) or for a related secondary purpose that would be reasonably expected or consented.

Our primary uses of personal information include but are not limited to:

- providing education, pastoral care, extra-curricular and health services;
- satisfying our legal obligations including our duty of care and child protection obligations;
- keeping parents informed as to the College community matters through correspondence, newsletters and magazines;
- marketing, promotional and fundraising activities;
- supporting the activities of College groups and associations including distribution of a parent's contact details on a class contact list and student contact details to Mount St Benedict Ex-Students' Association (MSBESA);
- supporting community based causes and activities, charities and other causes in connection with the College functions or activities;
- helping the College to improve our day to day operations including training our staff, systems development, developing new programs and services, undertaking planning, research and statistical analysis;
- school administration including for insurance purposes;
- the employment of staff and engagement of contractors and volunteers.

The College only uses personal information for the purposes for which it was provided, or for purposes which are related (or directly related in the case of sensitive information) to one or more of the function/activities listed above. The College may disclose personal information to government agencies, the Catholic Education Commission, Catholic Commission for Employment Relations, medical practitioners, other parents, other schools, recipients of College publications, visiting teachers, counselors and coaches, our service providers, agents, contractors, business partners and other recipients from time to time, only if one or more of the following apply:

- there is consent;
- it is reasonably expected that the College use or disclose personal information in this way;
- the College is authorized or required to do so by law;
- disclosure will lessen or prevent a serious threat to the life, health and safety of an individual or to public safety;
- where another permitted general situation or permitted health situation exception applies;
- disclosure is reasonably necessary for a law enforcement related activity.

Sensitive information has a higher degree of protection and will be used and disclosed only for the purpose for which it was provided, or for a directly related secondary purpose, unless the person agrees otherwise, or the use or disclosure of the sensitive information is required by law.

The College only collects sensitive information reasonably necessary for one or more of the functions/activities listed above if we have consent of the individuals to whom the sensitive information relates, or if the collection is necessary to lessen or prevent a serious threat to life, health or safety, or another permitted general situation (such as locating a missing person) or permitted health situation (such as the collection of health information to provide to health service) exists. If the College does not have the relevant consent and a permitted health situation or permitted general situation does not exist, then we may still collect sensitive information provided it relates solely to individuals who have regular contact with the College in

connection with our activities. The individuals may include students, parents, volunteers, former students and other individuals with whom the College has regular contact in relation to our activities.

The College may disclose personal information about an individual to overseas recipients in certain circumstances, such as when organizing an overseas excursion, facilitating a student exchange, or storing information with a "cloud computing service" which stores data outside of Australia. The College will however take all reasonable steps not to disclose an individual's personal information to overseas recipients unless it:

- has the individual's consent (which may be implied); or
- has satisfied ourselves that the overseas recipient is compliant with the Australian Privacy Principals, or a similar privacy regime; or
- has formed the opinion that the disclosure will lessen or prevent a serious threat to the life, health or safety of an individual or to public safety; or
- is taking appropriate action in relation to suspected unlawful activity or serious misconduct.

Personal information of Students

The Privacy Act does not differentiate between adults and children and does not specify an age after which individuals can make their own decisions with respect to their personal information. At Mount St Benedict College we take a common sense approach to dealing with a student's personal information and generally will refer any requests for personal information to a student's parents/carers. The College will treat notices provided to parents/carers as notices provided to students and will treat consents provided by parents/carers as consents provided by a student.

The College are however cognisant of the fact that children do have rights under the Privacy Act, and that in certain circumstances (especially when dealing with older students and especially when dealing with sensitive information), it will be appropriate to seek and obtain consents directly from students. The College also acknowledges that there may be occasions where a student may give or withhold consent with respect to the use of their personal information independently from their parents/carers. There may also be occasions where parents/carers are denied access to information with respect to their children, because to provide such information would have an unreasonable impact on the privacy of others, or result in a breach of the College's duty of care to the student.

Access to personal information

Under the Privacy Act and Health Records 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, therefore, parents may seek access to personal information collected about them and their daughter by contacting the College, students may also seek access to personal information about them. However, there are some exceptions to these rights set out in the applicable legislation, therefore, there may be occasions when access is denied. Such occasions would include situations such as (though not limited to) where access would have an unreasonable impact on the privacy of another, where access may result in a breach of the College's duty of care to the students or where students have provided information in confidence.

Requests for access to information, or to amend information held by the College, should be directed to the Principal in writing.

The College takes all reasonable steps to ensure the personal information it holds, uses and discloses is accurate, complete and up to date. These steps include ensuring that the personal information is accurate, complete and up to date at the time of collection and when using or disclosing the personal information. On an ongoing basis the College maintains and updates personal information when advised by individuals or when we become aware through other means that their personal information has changed. Please contact the College if any of the details that have been provided to the College have changed. You should also contact the College if you believe that the information we have about you is not accurate, complete or up to date.

Storage and Security of Personal Information

The College stores personal information in a variety of formats including on databases, in hard copy files and on personal devices including laptop computers, mobile phones, cameras and other recording devices.

The College staff are required to respect the confidentiality of students' and parents' personal information and the privacy of individuals.

The security of your personal information is of importance to the College and we will take all reasonable steps to protect the personal information held from misuse, loss, unauthorised access, modification or disclosure.

These steps include:

- restricting access to information on the College databases on a need to know basis with different levels of security being allocated to staff based on their roles and responsibilities and security profile
- ensuring all staff are aware that they are not to reveal or share personal passwords
- ensuring where sensitive information and health information is stored in hard copy files that these files are stored in lockable filing cabinets in lockable rooms. Access to these records is restricted to staff on a need to know basis
- implementing physical security measures around the College buildings and grounds to prevent break-ins
- implementing ICT security systems, policies and procedures, designed to protect personal information storage on our computer networks
- implementing human resources policies and procedures, such as email and internet usage, confidentiality and document security policies, designed to ensure that staff follow correct protocols when handing personal information
- undertaking due diligence with respect to third party service providers who may have access to personal information, including cloud service providers, to ensure as far as practicable that they are compliant with the Australian Privacy Principles or a similar privacy regime

Personal information held that is no longer needed is destroyed in a secure manner, deleted or de-identified as appropriate.

Our website may contain links to other websites. The College does not share your personal information with those websites and is not responsible for their privacy practices. Please check their privacy policies.

Privacy Complaints

If you wish to make a complaint about a breach by the College of the Australian Privacy Principles or the Health Privacy Principles you may do so by providing your written complaint by email, letter or by personal delivery to the Principal. You may also make a complaint verbally. The College will investigate any complaint and will respond within a reasonable time. The College may seek further information from you in order to provide a full and complete response. Your complaint may also be taken to the Office of the Australian Information Commissioner.

Notifiable Data Breach Scheme

A Notifiable Data Breach (NDB) is defined as a data breach, such as when personal information is lost or subjected to unauthorized access, modification, use or disclosure or other misuse, that is likely to result in serious harm to any of the individuals to whom the information relates. Serious harm includes serious physical, emotional, economic and financial harm as well as serious harm to reputation. Examples of circumstances which may meet the criteria of a NDB include a database containing personal information being hacked or personal information being mistakenly provided to the wrong person, records containing student information is stolen from unsecured recycling bins or disclosing personal information about students/staff for purposes other than what it what collected for and without the consent of the affected students/staff.

If an eligible data breach is suspected or believed to have occurred, the College must carry out a risk assessment. Once the a view is formed, based on reasonable grounds, that there has been a NDB, the College must prepare a statement of prescribed information in accordance with the Act, submit the statement to the Office of the Australian Information Commissioner by the use of an online form known as a Notifiable Data Breach Statement and contact all affected individuals directly or indirectly by publishing information about the NDB on publically accessible forums. The notification must include recommendations about the steps individuals should take in response to the breach.

March 2018	March 2021
Ratified by the College Board	Date for Review

DATA BREACH RESPONSE PLAN

1. This Data Breach Response Plan sets out the procedure to be followed by Mount St Benedict College staff in the event that the College experiences a data breach, or suspects that a data breach has occurred.
2. A data breach occurs when personal information is lost or subjected to unauthorised access, modification, use or disclosure or other misuse. Personal information refers to information that identifies or reasonably identifies an individual.
3. A data breach will also occur where protected College information is unlawfully used or disclosed.
4. Whilst the process outlined in this Data Breach Response Plan applies to all data breaches it is important to note that in some instances, the secrecy provisions may impose stricter standards on the College than those contained in this Response Plan. Thus, where a breach involves 'protected College information' both the Response Plan and the legislation must be considered collectively.
5. It is also important to note that Office of the Australian Information Commissioner (OAIC) is only concerned with breaches that involve personal information. Data breaches that involve 'protected College information' that is not 'personal information' do not need to be reported to the OAIC.
6. Adherence with the Response Plan will ensure the College can contain, assess and respond to data breaches in a timely fashion in order to mitigate potential harm to affected persons.
7. This plan:
    a. sets out the roles and responsibilities of staff;
    b. sets out the contact details of appropriate staff in the event of a data breach; and
    c. outlines the procedure to be followed in the event of a data breach.

Mount St Benedict College Staff member to notify College Principal or delegate

8. Immediately notify the College Principal or delegate of the suspected data breach.
9. Record and advise the College Principal or delegate of the time and date the suspected breach was discovered, the type of information involved, the cause and extent of the breach, and the context of the affected information and the breach.

Principal or delegate to assess the breach

10. The Principal or delegate must assess and determine whether a data breach has occurred.
11. If the Principal has any suspicion that a breach has occurred, she must assess the seriousness of the breach
12. In some instances, a minor breach may be able to be dealt with at the Principal level. Where a minor breach is dealt with at the Principal level, the following details must be recorded:
    a. description of the breach or suspected breach;
    b. action taken by the Principal or Mount St Benedict College staff member to address the breach or suspected breach;
    c. outcome of that action;
    d. sign off from the Principal that no further action is required; and
    e. confirmation that the incident has been recorded in the Mount St Benedict College Data breach incident log.
13. If the breach is serious, it must immediately be escalated to the Data Breach Response Team.

Data Breach Response Team Contact persons:

14. The Response Team includes:
    a. Principal or delegate
    b. Head of ICT
    c. Marketing Manager
    d. Business Manager
15. It is not necessary that all members of the Response Team be included in all data breach responses.

Process:

16. Each breach will need to be dealt with on a case-by-case basis, undertaking an assessment of the risks involved and using that risk assessment as the basis for deciding what actions to take in the circumstances.
17. There are four key steps to consider when responding to a breach or suspected breach.

Step 1: Contain the breach and do a preliminary assessment

Contain the breach

18. Once a data breach has been identified, action must be taken to immediately contain it. For example, stop the unauthorised practice, recover the records or shut down the system that was breached.

Initiate a preliminary assessment

19. Move quickly to designate a person/team to coordinate the response and lead the initial investigation. In some instances, this may be a member of the Response Team. In other instances, it will be a person/s most suitably qualified to carry out the initial investigation (as determined by the Response Team).
20. The following questions should be addressed when making the preliminary assessment:
    a. What information does the breach involve?
    b. What was the cause and extent of the breach?
    c. What are the harms (to affected persons) that could potentially be caused by the breach?
    d. How can the breach be contained?

Step 2: Evaluate the risks associated with the breach

21. The following factors are relevant when assessing the risk:
    a. The type of information involved
        i. Is it personal information or protected College information?
        ii. Does the type of information create a greater risk of harm?
        iii. Who is affected by the breach?
    b. Determine the context of the affected information and the breach
        i. What is the context of the information involved?
        ii. What parties have gained unauthorised access to the affected information?
        iii. Have there been other breaches that could have a cumulative effect?
        iv. How could the information be used?
    c. Establish the cause and extent of the breach
        i. Is there a risk of ongoing breaches or further exposure of the information?
        ii. Is there evidence of theft?
        iii. Is the information adequately encrypted, anonymised or otherwise not accessible?
        iv. What was the source of the breach? (risk of harm may be lower where source of the breach is accidental rather than intentional)
        v. Has the information been recovered?
        vi. What steps have already been taken to mitigate the harm?
        vii. Is this a systemic problem or an isolated incident?
        viii. How many persons are affected by the breach?
    d. Assess the risk of harm to the affected persons
        i. Who is the recipient of the information?
        ii. What harm to persons could result from the breach?
    e. Assess the risk of other harms
        i. Other possible harms, including to the agency or organisation that suffered the breach, e.g:
            1. The loss of public trust in the agency
            2. Reputational damage
            3. Legal liability
            4. Breach of secrecy provisions
22. A thorough evaluation of the risks will assist the College in determining the appropriate course of action to take.

Step 3: Notification

Deciding whether to notify affected individuals or entities

23. In general, if a data breach creates a real risk of serious harm to a person, the affected person should be notified.
24. The key consideration is whether notification is necessary to avoid or mitigate serious harm to an affected person.
25. Consider the following factors:
    a. What is the risk of serious harm to the person as determined by step 2?
    b. What is the ability of the person to avoid or mitigate possible harm if notified of a breach (in addition to steps taken by the agency or organisation)?
    c. Even if the person would not be able to take steps to fix the situation, is the information that has been compromised sensitive or likely to cause humiliation or embarrassment?
    d. What are the legal and contractual obligations to notify and what are the consequences of notification?

Notification process

26. In general, notification should occur as soon as reasonably possible.
27. Notification should be direct – by phone, letter, email or in person, to the affected individuals.
28. Indirect notification, either by website, posted notices or media should only occur where direct notification could cause further harm, is cost prohibitive or the contact information for affected persons is unknown.

Details to include in the notification

29. The content of the notification will vary depending on the particular breach and notification method. However, the OAIC recommend that notifications should include the following information:
    a. incident description;
    b. type of information involved;
    c. response to the breach;
    d. assistance offered to affected persons;
    e. other information sources designed to assist in protecting against identity theft or interferences with privacy (e.g. www.oaic.gov.au);
    f. the College contact details;
    g. whether breach notified to regulator or other external contact(s);
    h. legal implications (e.g. the secrecy provisions);
    i. how individuals can lodge a complaint with the College; and
    j. how individuals can lodge a complaint with the OAIC (where the information is personal information).

Other notifications

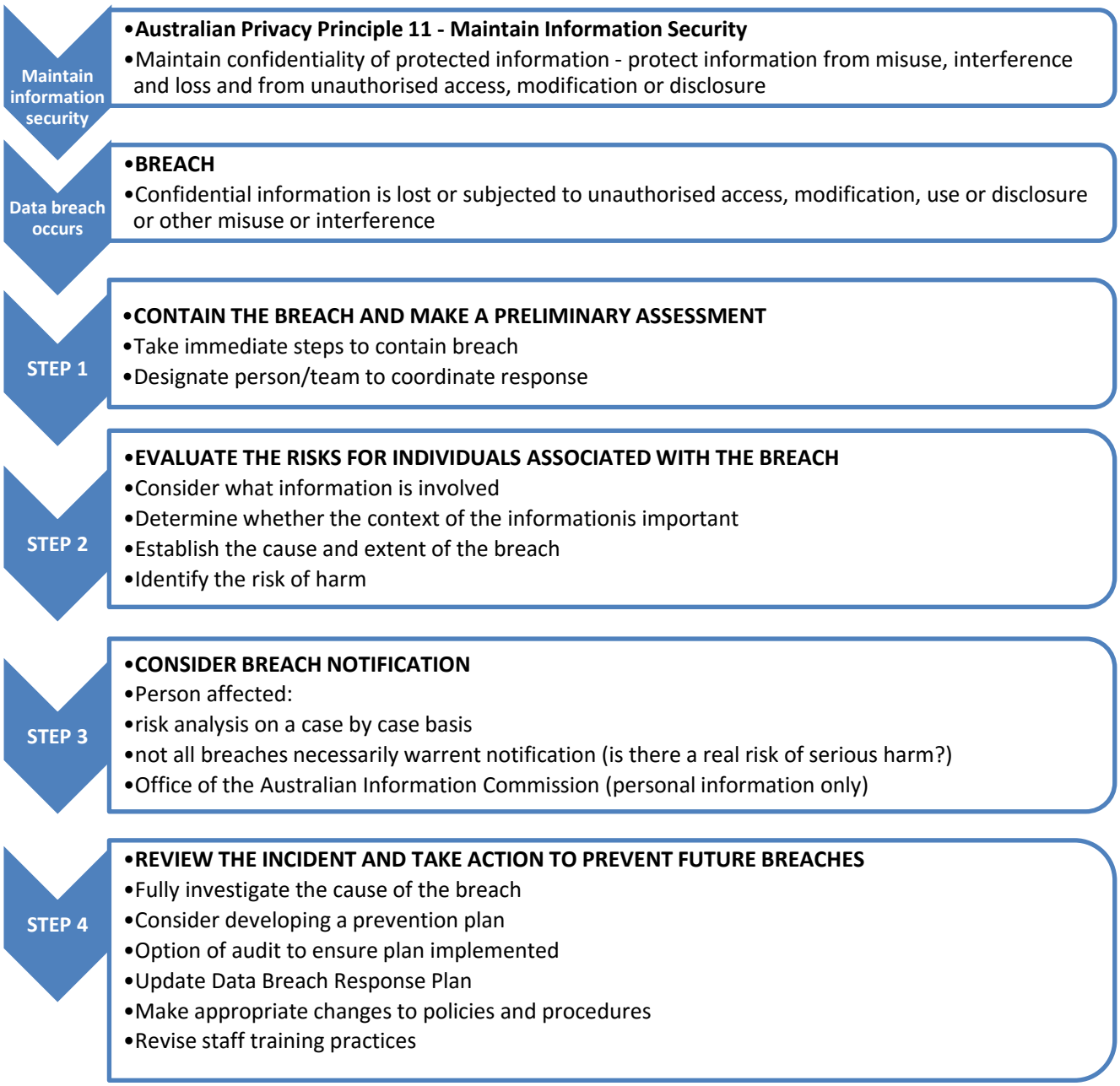
30. It may also be appropriate to notify other third parties, such as:
    a. The OAIC.
    b. The Police.
    c. Insurance providers.
    d. Credit card companies, financial institutions.
    e. Professional or other regulatory bodies.
    f. Other internal or external parties who have not already been notified.
    g. Agencies that have a direct relationship with the information lost/stolen.

31. The OAIC strongly encourages agencies to report serious data breaches involving personal information. The following factors should be considered in deciding whether to report a breach to the OAIC:
    a. any applicable legislation that may require notification;
    b. the type of personal information involved and whether there is a real risk of serious harm arising from the breach;
    c. whether a large number of people were affected by the breach;

d. whether the information was fully recovered without further disclosure;
e. whether the affected individuals have been notified; and
f. if there is a reasonable expectation that the OAIC may receive complaints/inquiries about the breach.

Step 4: Prevent future breaches.

32. Once immediate steps have been taken to mitigate the risks associated with a breach, the College must take the time to investigate the cause of the breach.
33. The College Executive Leadership Team must be briefed on the outcome of the investigation, including recommendations:
    a. to make appropriate changes to policies and procedures if necessary;
    b. revise staff training practices if necessary; and
    c. update this Response Plan if necessary.



Mount St Benedict College

COLLECTION NOTICE UNDER THE PRIVACY ACT

1. Mount St Benedict College collects personal information, including sensitive information about students and parents or guardians before and during the course of a student's enrolment at the College. This may be in writing or in the course of conversations. The primary purpose of collecting this information is to enable the College to provide appropriate educational opportunities to the pupil and to enable her to take part in all the activities of the College.
2. Some of the information we collect is to satisfy the College's legal obligations, particularly to enable the College to discharge its duty of care.
3. Laws governing or relating to the operation of schools require certain information to be collected and disclosed. These include relevant Education Acts, and Public Health and Child Protection laws.
4. Health information about pupils is sensitive information within the terms of the Australian Privacy Principles under the Privacy Act. The College may ask you to provide medical reports about pupils from time to time.
5. The College from time to time discloses personal and sensitive information to others for administrative and educational purposes including facilitating the transfer of a student to another school. This includes other schools, government agencies, Catholic Education Commission, medical practitioners, and people providing services to the College, including specialist visiting teachers, [sports] coaches, counsellors and volunteers.
6. If the College does not obtain the information referred to above we may not be able to enrol or continue the enrolment of the student.
7. Personal information collected from students is regularly disclosed to their parents or guardians.
8. The College may store personal information in the "cloud" which may mean that it resides on servers which are situated outside Australia.
9. Parents may seek access to personal information collected about them and their daughter(s) by contacting the College. Students may also seek access to personal information about themselves. However, there will be occasions when access is denied. Such occasions would include 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 students, or where students have provided information in confidence.
10. As you may know the College from time to time engages in fundraising activities. Information received from you may be used to request your support. It may also be disclosed to organisations that assist in the College's fundraising activities solely for that purpose. The College will not disclose your personal information to third parties for their own marketing purposes without your consent.
11. On occasions information such as academic and sporting achievements, student activities and other news is published in College newsletters, magazines and on our website. Photographs of student activities such as sporting events, school camps and school excursions may be taken for publication in the College newsletters and magazines. The College will obtain separate permissions from the student's parent or guardian prior to publication if we would like to include photographs or other identifying material in promotional material for the College or otherwise make it available to the public such as on the internet.
12. The Archives department will, on occasion, publish photographs of ex-students on the College's website, social media pages, newsletters, magazines, displays and history publications.
13. The College may include student and parent contact details in a Homeroom list to the respective Class Parents.
14. If you provide the College with the personal information of others, such as doctors' or emergency contacts, you are encouraged to inform them that you are disclosing that information to the College and why, so that they can access that information if they wish and that the College does not usually disclose the information to third parties.
15. The College Privacy Policy also sets out how you may complain about a breach of privacy and how the College will deal with such a complaint.
16. If the College forms the view, based on reasonable grounds, that there has been a Notifiable Data Breach, the College will notify the Office of the Australian Information Commissioner by use of an online form known as a Notifiable Data Breach Statement as well as individuals whose personal information is likely to result in serious harm due to the breach as soon as practicable?

Feb 2009, Amended Feb 2011, Oct 2014, Mar 2015, Sept 2017, Feb 2018

May 2010, Amended October 2014, September 2017, February 2018