Adopted by College Council
Date: August 2017
Last Review: May 2017

PRIVACY POLICY

Including Data Breach Response Procedure

Purpose of this Policy
This policy outlines the Melton Christian College (MCC) practices on how the College uses and manages personal information provided to or collected by it. MCC is bound by the National Privacy Principles (NPP) contained in the *Commonwealth Privacy Act 1998*.

Updating this Policy
MCC may, from time to time, review and update this Privacy Policy to take account of new laws and technology, changes to College operations and practices, and to make sure it remains appropriate in respect of MCC being a Christian school expressly founded for the purpose of providing Christian education for those families who wish to choose that for their children.
If MCC decides to change its practice in relation to privacy and the management of personal information, it will make those changes in this privacy statement which is its Privacy Policy.

What kind of information does the Melton Christian College collect and how is it collected?
The type of information MCC collects and holds includes (but is not limited to) personal information, it is acknowledged that some such information may be considered to be 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; and
- other people who come into contact with the College.

Personal Information individuals or families provide: MCC will generally collect personal information held about an individual by way of hard-copy or soft-copy forms filled out by Parents or pupils, face-to-face meetings and interviews, other soft-version data collection, and telephone calls. On occasions people other than Parents and pupils provide personal information.

Personal Information provided by other people: In some circumstances MCC 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.

Exception in relation to employee records: The NPPs 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.

How will Melton Christian College use the personal information that people provide?
MCC will use personal information it collects for the primary purpose of collection, and for such other secondary purposes that are related to the primary purpose of collection and reasonably expected, or to which the provider has consented.

Pupils and Parents: In relation to personal information of pupils and Parents, MCC's primary purpose of collection is to enable the College to provide schooling for the pupil. This includes satisfying both the needs of Parents and needs of the pupil throughout the whole period the pupil is enrolled at MCC.
The purposes for which MCC uses personal information of pupils and Parents include:

- to keep Parents informed about matters related to their child's schooling, through correspondence, whether digital or hard-copy, newsletters and magazines;
- day-to-day administration;
- looking after pupils' educational, social and medical wellbeing;
- seeking donations and marketing for MCC;
- to satisfy MCC's legal obligations and allow the College to discharge its duty of care.

In some cases where MCC requests personal information about a pupil or Parent, if the information requested is not obtained, the College may not be able to enrol or continue the enrolment of the pupil.

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 MCC 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 MCC;
- to satisfy MCC's legal obligations, for example, in relation to child protection legislation.

Volunteers: MCC also obtains personal information about volunteers who assist the College in its functions or conduct associated activities, to enable the College and the volunteers to work together.

Marketing and fundraising: MCC 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 be a quality learning environment in which both pupils and staff thrive. Personal information held by MCC may be disclosed to an organisation that assists in the College's fundraising.
Parents, staff, contractors and other members of the wider School community may from time to time receive fundraising information. MCC publications, like newsletters and magazines, which include personal information, may be used for marketing purposes via soft or hard media.

Who might Melton Christian College disclose personal information to?
MCC may disclose personal information, including potentially sensitive information, held about an individual to:

- another school;
- government departments;
- medical practitioners;
- people providing services to the College, including specialist visiting teachers, testing agencies and sports coaches;
- recipients of College publications, like newsletters and magazines;
- parents; and
- anyone that the provider of the information authorises MCC to disclose information to.

Sending information overseas: apart from the obvious reality that websites and certain other digital forms of passive distribution of information can be accessed anywhere without international limitations, MCC will not actively 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 National Privacy Principles.

How does Melton Christian College treat sensitive information?
In referring to 'sensitive information', the College means: information relating to a person's racial or ethnic origin, political opinions, religion, trade union or other professional or trade association membership, sexual preferences or criminal record, that is also personal information; and health information about an individual.

Sensitive information will be used and disclosed only for the purposes 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 required by law.

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.

MCC has in place steps to protect the personal information the College holds from misuse, loss, unauthorised access, modification or disclosure by us of various methods including locked storage of hard-copy records and digitally secured access to soft-copy records.

Updating personal information

MCC endeavours to ensure that the personal information it holds is accurate, complete and up-to-date. A person may seek to update their personal information held by the College by contacting the office of the College at any time.

Disposing of Information

The National Privacy Principles require MCC not to store personal information longer than necessary and personal information no longer required by the College will be disposed of securely.

An individual has the right to check what personal information Melton Christian College holds about them.

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. 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, whenever appropriate Parents will be informed. Notwithstanding that, this policy acknowledges that sometimes situations arise when College staff may reasonable suspect that abuse or other criminal activity may mean it is important for a student's confidentiality to be maintained. In such an instance it is most likely that a child protection agency be contacted also.

To make a request to access any information MCC holds about you or your child, please contact the Principal in writing or by email.

MCC 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.

Consent and rights of access to the personal information of pupils

MCC respects every Parent's right to make decisions concerning their child's education.

Generally, MCC 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.

Parents may seek access to personal information held by MCC about them or their child by contacting the office. 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.

MCC 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.

Website and Digital Information

MCC collects and use information throughout our website only within the guidelines as explained in this Privacy Policy.

MCC gathers two types of information about users. Firstly, information that users provide through optional, voluntary submissions. For example, there are voluntary submissions to receive the College newsletters or contact forms via the MCC website. Secondly, information MCC gathers through aggregated tracking

information derived mainly by tallying page views throughout our sites. This information allows us to better tailor our content to readers' needs and to better understand the demographics of our users. MCC may track user patterns of the website. However, MCC does not correlate this information with data about individuals. Under no circumstances does Melton Christian College divulge any information about an individual user to a third party, except to comply with applicable law or valid legal process or to protect the personal safety of our users or the public. The information we collect is never shared with other organisations for commercial purposes, and only used to provide more relevant content and to make our site more user-friendly. Consistent with the Commonwealth Privacy Act and National Privacy Principles, MCC will never knowingly request personally identifiable information from anyone under the age of 13 without requesting parental consent.

Use of information

Melton Christian College uses any information voluntarily given by our users to enhance their experience in our network of sites, whether to provide interactive or personalized elements on the sites or to better prepare future content based on the interests of our users.

DATA BREACH RESPONSE PROCEDURE

Definition of a data breach

A data breach occurs when personal information held by the College is lost, subjected to unauthorized access, modification, disclosure, or other misuse or interference.

Examples may include:

- Devices or items capable of storing data such as discs, hard drives, keys, etc being discarded while still containing accessible data, and hard-copy material being accessed inappropriately from recycling or waste
- Devices that hold data such as laptops, removable storage devices, keys, hard-copy registers being lost or stolen
- Mistaken provision of data such as details or information being erroneously sent by email or hard-copy to the wrong recipient. This may be caused by malicious and deceptive approach by an individual with the result that the College into improperly and inadvertently releases data
- Staff accessing, utilizing or disclosing data in ways that are outside the requirements or authority of their position
- Systems or databases being accessed; without authorisation, hacked, illegally or inappropriately accessed in some other way by individuals inside or outside of Melton Christian College

Data breach response steps

1. Immediately assess the breach
2. To the extent possible immediately contain the breach
3. Immediately notify ICT Manager and Business Manager
4. Business Manager and ICT Manager will notify Principal
5. Depending on the assessment of the breach, Principal may notify Director(s) and respond further by enacting the next steps of wider notifications

The initial step is that the extent of the breach needs to be diagnosed. This may mean assessment by ICT Technicians and/or ICT Manager. With priority commitment to speedy response, under the guidance of the ICT Manager and his/her team, the steps necessary to contain the breach are to be taken immediately. Thus the breach is to be arrested as soon as possible so that any continued access to data is halted.

Once the breach has been initially assessed, then initially contained and further resultant losses prevented, the next step is:

6. Measure risks associated with the breach. Here are suggestions as to measuring associated risk
    a. What is the nature of the personal information that has been compromised?
    b. How was the security of the data breached?
    c. What is the magnitude of the breach, who is affected, and to what extent?
    d. What is the nature of the damage that the breach may cause?
    e. How best can the breach be contained, is it currently contained, and what needs to be done in order for it to be contained?

Notifications

7. There is to be a crucial evaluation of the need to notify and the means and reach of the notification:
    a. Do we notify individuals affected by the breach?
    b. Do we notify individuals unaffected by the breach, but who will find out about it through other means?
    c. What is the most effective means of notification?
    d. Will that form of communicating the breach make the College vulnerable to other risks?
    e. What is the most reputation-protecting way to notify of the breach?
    f. Should the notification be from the organisation (unsigned off) or from an individual representing the organisation (eg Principal)?
    g. Who should be notified, and in what capacity are they to be notified?

h. What information should be included when notifying? Should it include:
    i. Description of how the breach happened, eg, theft, loss, hacking
    ii. Type of personal information that may have been exposed
    iii. Our initial response as an organisation
    iv. What we will offer in terms of support or practical help

Protocols contributing to Prevention of Data Breaches

- Provide information and reminders to volunteers of their need to interact appropriately with information of any kind that is held by or relates to MCC
- Provide training and reminders to staff in relation to these procedures
- Refresh passwords systematically and periodically
- Review and update these Data Breach Response Procedures
- Safeguard that data and soft versions of documents are securely, appropriately and lawfully destroyed
- Safeguard that data as well as data storage devices are securely and appropriately stored
- Safeguard that devices including portable devices are securely, appropriately and lawfully destroyed
- Safeguard that hard-copy documents are securely, appropriately and lawfully destroyed

Subject the Privacy Policy to periodic review and Procedure.