

Privacy Policy

This Privacy Policy sets out how Mercy Regional College manages personal information provided to or collected by it.

Mercy Regional College is bound by the Australian Privacy Principles contained in the Commonwealth *Privacy Act 1988*. In relation to health records, Mercy Regional College is also bound by the *Health Records Act 2001* (Vic.) and the Health Privacy Principles in that Act.

Mercy Regional College may, from time to time, review and update this Privacy Policy to take account of new laws and technology, changes to the School's operations and practices and to make sure it remains appropriate to the changing school environment.

What kinds of personal information does Mercy Regional College collect and how does the School collect it?

Mercy Regional College collects and holds personal information, including health and other sensitive information, about:

- pupils and parents and/or guardians ('Parents') before, during and after the course of a pupil's enrolment at Mercy Regional College including:
 - name, contact details (including next of kin), date of birth, previous school and religion
 - medical information (e.g. details of disability and/or allergies and details of any assistance the student receives in relation to those disabilities)
 - conduct and complaint records, or other behaviour notes, school attendance and school reports
 - information about referrals to government welfare agencies
 - counselling reports
 - health fund details and Medicare number
 - any court orders
 - volunteering information (including Working With Children Checks)
 - photos and videos at school events.
- job applicants, staff members, volunteers and contractors, including:
 - name, contact details (including next of kin), date of birth and religion
 - information on job application
 - professional development history
 - salary and payment information, including superannuation details
 - medical information (e.g. details of disability and/or allergies and medical certificates)
 - complaint records and investigation reports
 - leave details
 - photos and videos at school events
 - work emails and private emails (when using work email address) and internet browsing history
 - the banking, credit card or financial information of staff, families & creditors

Personal Information you provide: Mercy Regional College will generally collect personal information held about an individual by way of forms filled out by parents or pupils, face-to-face meetings and interviews, emails and telephone calls.

Personal Information provided by other people: In some circumstances Mercy Regional College may be provided with personal information about an individual from a third party, for example a report provided by a medical professional or a reference from another school.

Exception in relation to employee records: Under the *Privacy Act*, the Australian Privacy Principles do not apply to an employee record. As a result, this Privacy Policy does not apply to Mercy Regional College'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 2001 (Vic.)*.

Anonymity: Mercy Regional College needs to be able to identify individuals with whom it interacts and to collect identifiable information about them to facilitate the delivery of schooling to its students and its educational and support services, conduct the job application process and fulfil other obligations and processes. However, in some limited circumstances some activities and interactions with Mercy Regional College may be done anonymously where practicable, which may include making an inquiry, complaint or providing feedback.

How will the School use the personal information you provide?

Mercy Regional College will use personal information it collects from you for the primary purpose of collection, and for such other secondary purposes that are related to the primary purpose of collection and reasonably expected by you, or to which you have consented.

Pupils and Parents: In relation to personal information of students and parents, Mercy Regional College's primary purpose of collection is to enable the College to provide schooling to pupils enrolled at Mercy Regional College (including educational and support services for the student), exercise its duty of care and perform necessary associated administrative activities.

The purposes for which the College uses personal information of students and Parents include:

- to keep parents informed about matters related to their child's education, through correspondence, newsletters and magazines;
- day-to-day administration;
- looking after students' educational, social and medical wellbeing;
- for marketing and fundraising purposes.
- to satisfy the College's legal obligations and discharge its duty of care
- to satisfy Mercy Regional College's service providers' legal obligations, including the Catholic Education Commission of Victoria Ltd (CECV) and the Catholic Education Offices.

In some cases where Mercy Regional College requests personal information about a student or parent; if the information requested is not provided, Mercy Regional College may not be able to enrol or continue the enrolment of the pupil or permit the pupil to take part in a particular activity.

Job applicants and contractors: In relation to personal information of job applicants 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 Mercy Regional College uses personal information of job applicants, staff members and contractors include:

- administering the individual's employment or contract, as the case may be
- for insurance purposes
- seeking donations and marketing for the School
- satisfying the School's legal obligations, for example, in relation to child protection legislation.

Volunteers: Mercy Regional College also obtains personal information about volunteers who assist the School in its functions or conduct associated activities, to enable the School and the volunteers to work together and to confirm their suitability and to manage their visits.

Counsellors: Mercy Regional College contracts with external providers to provide counselling services for some pupils. The principal may require the Counsellor to inform him or her or other teachers of any

issues the principal and the Counsellor believe may be necessary for the School to know for the well-being or development of the pupil who is counselled or other pupils at Mercy Regional College.

Marketing and fundraising: Mercy Regional College regards marketing and fundraising as an important part of ensuring that Mercy Regional College continues to provide a quality learning environment. Personal information held by the School may be disclosed to organisations that assist in the School's fundraising, for example, Mercy Regional College Parent's Association [or, on occasions, external fundraising organisations].

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

Who might Mercy Regional College disclose personal information to and store your information with?

Mercy Regional College may disclose personal information (including sensitive information) held about an individual for **educational, administrative and support purposes**. This may include:

- School service providers which provide educational, support and health services to Mercy Regional College, (either at Mercy Regional College or off campus) including the Catholic Education Commission of Victoria Ltd (CECV), Catholic Education Offices, specialist visiting teachers, volunteers, counsellors and providers of learning and assessment tools
- third party service providers that provide online educational and assessment support services, document and data management services, or applications to schools and school systems including the Integrated Catholic Online Network (ICON) and Google's G Suite, including Gmail and, where necessary, to support the training of selected staff in the use of these services
- other third parties which the school uses to support or enhance the educational or pastoral care services for its pupils or to facilitate communications with parents
- another schools including to its teachers to facilitate the transfer of a pupil
- State and Federal government departments and agencies
- health service providers
- recipients of College publications, such as newsletters and magazines
- pupils, parents or guardians and their emergency contacts
- assessment and educational authorities including the Australian Curriculum, Assessment and Reporting Authority
- anyone who we are required or authorised to disclose the information to by law, including child protection laws.

Nationally Consistent Collection of Data (NCCD) on School Pupils with Disability

Mercy Regional College is required by the Federal *Australian Education Regulation 2013* to provide certain information under the NCCD on pupils with a disability. Mercy Regional College provides the required information to the CECV, as an approved authority, to provide on the school's behalf. Under the NCCD, the following information is required for each pupil with a disability:

- their level of education (i.e. primary or secondary)
- their category of disability (i.e. physical, cognitive, sensory or social/emotional)
- their level of adjustment (i.e. support provided within quality differentiated teaching practice, supplementary, substantial or extensive adjustment).

Pupil information provided for the purpose of the NCCD does not explicitly identify any pupil. However, Mercy Regional College will disclose pupil's names to the CECV, to enable CECV to undertake financial modelling about funding for pupil's, including ongoing evaluation of the adequacy of the funding for individual pupils under the NCCD. The CECV will not disclose a pupil's identity for the NCCD.

Sending and storing information overseas: Mercy Regional College may disclose personal information about an individual to overseas recipients, for instance, to facilitate a school exchange. However, the School will not send personal information about an individual outside Australia without:

- obtaining the consent of the individual; or
- otherwise complying with the Australian Privacy Principles or other applicable privacy legislation.

Mercy Regional College may also store personal information in the 'cloud'. This means that the information is held on the servers of third party cloud service providers engaged by Mercy Regional College. The servers are situated in or outside of Australia.

Mercy Regional College may from time to time use the services of third party online service providers (including for the delivery of services and third party online applications, or Apps relating to email, instant messaging and education and assessment, such as Google's G Suite, including Gmail) which may be accessible by you. Some personal information may be collected and processed or stored by these providers in connection with these services. These online service providers may be located in or outside Australia.

School personnel and Mercy Regional College service providers, and the CECV and its service providers, may have the ability to access, monitor, use or disclose emails, communications (e.g. instant messaging), documents and associated administrative data for the purposes of administering the system and services ensuring their proper use.

As not all countries are bound by laws which provide the same level of protection for personal information provided by the APPs, the School makes reasonable efforts to be satisfied about the security of any personal information collected, processed and stored outside Australia, including that of cloud and third party service providers.

Where personal and sensitive information is retained by a cloud service provider on behalf of CECV to facilitate Human Resources and staff administrative support, this information may be stored on servers located in or outside Australia.

How does Mercy Regional College treat sensitive information?

In referring to 'sensitive information', the School means: information relating to a person's racial or ethnic origin, political opinions, religion, trade union or other professional or trade association membership, philosophical beliefs, sexual orientation or practices or criminal record, that is also personal information; health information and biometric information about an individual.

Sensitive information will be used and disclosed only for the purpose for which it was provided or a directly related secondary purpose, unless you agree otherwise, or the use or disclosure of the sensitive information is allowed by law.

Management and security of personal information

Mercy Regional College staff are required to respect the confidentiality of pupil's and parents' personal information and the privacy of individuals.

Mercy Regional College has in place steps to protect the personal information the School holds from misuse, interference and loss, unauthorised access, modification or disclosure by use of various methods including locked storage of paper records and password access rights to computerised records. This includes responding to any incidents which may affect the security of the personal information it holds. If we assess that anyone whose information is affected by such a breach is likely to suffer serious harm as a result, we will notify them and the Office of the Australian Information Commissioner of the breach. It is recommended that parents and Mercy Regional Colleges' community adopt secure practices to protect themselves. You should ensure that all passwords you use are strong and regularly updated and that your log in details are kept secure. Do not share your personal information with anyone without first verifying their identity and organisation. If you believe any of your personal information has been compromised, please let the School know immediately.

Notifiable Data Breach Scheme

Changes to the Privacy Act 1988 (Cth) make it compulsory for schools and other organisations to notify specific types of data breaches to individuals affected by the breach, and to the Office of the Australian

Information Commissioner (OAIC). A data breach occurs when personal information is lost or subject to unauthorised access, modification, disclosure, or other misuse or interference.

Where a data breach has occurred that is likely to result in serious harm to any of the individuals to whom the information relates, it is considered 'eligible' and must be reported to the OAIC. Serious harm could include serious physical, physiological, emotional, economic and financial harm, as well as reputation.

Mercy Regional College follows procedures according to the Data Breach Response Plan. This requires that any breaches are reported to the principal and a risk assessment is conducted. If a serious breach is identified, then the principal completes *Data Breach Statement: What must be included*

Notification to the OAIC is only required if the consequences of a data breach are likely to cause serious harm. Examples of data breaches that may likely to cause series harm and include:

- loss or theft of a laptop or other device containing the personal information of pupil's or staff
- hacking of a database containing personal information
- mistaken provision of personal information to the wrong person.

Access and correction of personal information

Under the Privacy Act and the Health Records Act, an individual has the right to seek and obtain access to any personal information and health records respectively that Mercy Regional College holds about them and to advise the School of any perceived inaccuracy. Pupils will generally be able to access and update their personal information through their parents, but older pupils may seek access and correction themselves.

There are some exceptions to the access rights set out in the applicable legislation.

To make a request to access or to update any personal information Mercy Regional College holds about you or your child, please contact the Principal in writing. The School may require you to verify your identity and specify what information you require. The School 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 School will advise the likely cost in advance. If we cannot provide you with access to that information, we will provide you with written notice explaining the reasons for refusal.

Consent and rights of access to the personal information of students

Mercy Regional College 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. 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.

As mentioned above, parents may seek access to personal information held by the College about them or their child by contacting the Principal by telephone or by email. However, there may 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 School's duty of care to the pupil.

Mercy Regional College may, at its discretion, on the request of a pupil grant that pupil access to information held by the School 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 warrant it.

Enquiries and complaints and contact details

If you would like further information about the way Mercy Regional College manages the personal information it holds about you, or wish to complain that you believe that the School has breached its

privacy obligations, please contact the School Principal by writing or email. Mercy Regional College will investigate your complaint and will notify you of the making of a decision in relation to your complaint as soon as is practicable after it has been made.

If you are not satisfied with the School's decision you may make a complaint to the Office of the Australian Information Commissioner (OAIC) whose contact details are:

GPO Box 5218, Sydney, NSW 2001

Telephone: 1300 363 992

www.oaic.gov.au

References:

[Data Breach Notification Guide](#)

[Privacy Act 1988](#)

[Health Records Act 2001 \(Vic.\)](#)

[Catholic Education Commission of Victoria Ltd \(CECV\)](#)

[Federal Australian Education Regulation 2013](#)

[Standard Collection Notice](#)

Appendix 1. Standard Collection Notice

1. The College collects personal information, including sensitive information about students and parents or guardians and family members before and during the course of a student's enrolment at the College. This may be in writing or in the course of conversations and may be direct from the individual or from another source. The primary purpose of collecting this information is to enable the School, Catholic Education Offices and the Catholic Education Commission of Victoria Ltd (CECV) to meet its educational, administrative and duty of care responsibilities to the student to enable them to take part in all the activities of the School. The School makes reasonable efforts to be satisfied about the security of any personal information collected, processed and stored outside Australia, including that of cloud and third party service providers.
2. Some of the information the School collects is to satisfy the School's legal obligations, particularly to enable the School to discharge its duty of care.
3. Laws governing or relating to the operation of a school require certain information to be collected and disclosed. These include relevant Education Acts and Public Health and Child Protection laws.
4. Health information about students (which includes information about any disability) is sensitive information within the terms of the Australian Privacy Principles (APPs) under the *Privacy Act 1988*. The School may request medical reports about students from time to time and may otherwise collect sensitive information about students and their families.
5. If any personal information requested by the College is not provided, this may affect the College's ability to enrol a student, respond to enquiries, provide the student with educational and support services or allow a person to visit the College.
6. The College may disclose personal and sensitive information for **administrative, educational and support purposes** (or may permit the information to be directly collected by third parties). This may include to:
 - School service providers such as the CECV, Catholic Education Offices, school governing bodies and other dioceses
 - third party service providers that provide online educational and assessment support services or applications (apps), which may include email and instant messaging
 - School systems, including the Integrated Catholic Online Network (ICON) and Google's 'G Suite' including Gmail. Limited personal information such as student/individual learning plans may be collected and processed or stored by these providers in connection with these services
 - CECV to undertake financial modelling for students with a disability, including ongoing evaluation of funding adequacy for individual students
 - CECV to support the training of selected staff in the use of schools' systems, such as ICON
 - another school to facilitate the transfer of a student
 - Federal and State government departments and agencies
 - health service providers, and people providing educational support and health services to the College, including specialist visiting teachers, volunteers, counsellors and providers of learning and assessment tools

- assessment and educational authorities, including the Australian Curriculum, Assessment and Reporting Authority
 - people providing administrative and financial services to the College
 - anyone you authorise the College to disclose information to; and
 - anyone to whom the College is required or authorised to disclose the information to by law, including under child protection laws.
7. Personal information collected from students is regularly disclosed to their parents or guardians.
 8. The College may also use cloud computing service providers to store personal information (which may include sensitive information) on their servers in the 'cloud'. These servers may be located in or outside Australia. This may mean that personal information may be stored or processed outside Australia.
 9. As not all countries are bound by laws which provide the same level of protection for personal information as the APPs, the College makes reasonable efforts to be satisfied about the protection of any personal information that may be collected, processed and stored outside Australia in connection with any cloud and third party services.
 10. When the College uses Google's G-Suite including Gmail, some personal information (usually limited to name and email address) of students, parents or guardians may be transferred, stored and processed by Google in the United States, or in any other country through which Google provides these services or where it processes and stores information. This personal information will be stored and processed by Google in accordance with Google's terms and conditions stated in the G-Suite for Education Agreement which the school entered into with Google.
 11. The countries in which the servers of cloud service providers and other third party service providers may be located are:
 - United States
 - Netherlands
 - Ireland
 - Singapore
 - Hong Kong, China
 12. Where personal, including sensitive information is held by a cloud computing service provider on behalf of CECV for educational and administrative purposes, it may be stored on servers located within or outside Australia. This includes the ICON system.
 13. College personnel and the College's service providers, and the CECV and its service providers, may have the ability to access, monitor, use or disclose emails, communications (e.g. instant messaging), documents and associated administrative data for the purposes of administering the ICON system and ensuring its proper use.
 14. The College's Privacy Policy is accessible via the school website, newsletter, handbook, or from the College office. The policy sets out how parents, guardians or students may seek access to, and correction of their personal information which the College has collected and holds. However, access may be refused in certain circumstances such as where access would have an unreasonable impact on the privacy of others, or may result in a breach of the College's duty of care to the student, or where students have provided information in confidence. Any refusal will be notified in writing with reasons if appropriate.

15. The College's Privacy Policy also sets out how parents, guardians, students and their family can make a complaint if they believe the College has interfered with their privacy [and how the complaint will be handled].
16. The College may engage in fundraising activities. Information received from you may be used to make an appeal to you. We will not disclose your personal information to third parties for their own marketing purposes without your consent.
17. On occasions information such as academic and sporting achievements, student activities and similar news is published in School newsletters and magazines, on our intranet [and on our website]. This may include photographs and videos of student activities such as sporting events, school camps and school excursions. The College will obtain permissions from the student's parent or guardian (and from the student if appropriate) prior to publication to enable the school to include such photographs or videos [or other identifying material] in our promotional material or otherwise make this material available to the public such as on the internet. The College may obtain permissions annually, or as part of the enrolment process. Permissions obtained at enrolment may apply for the duration of the student's enrolment at the College unless the College is notified otherwise. Annually, the College will remind parents and guardians to notify the College if they wish to vary the permissions previously provided.
18. If you provide the College with the personal information of others, such as other family members, doctors or emergency contacts, we encourage you to inform them you are disclosing that information to the College and why, that they can request access to and correction of that information if they wish and to also refer them to the College's Privacy Policy for further details about such requests and how the College otherwise handles personal information it collects and complaints it receives.

Appendix 2.

Data Breach Response Plan

This data breach response plan sets out procedures in the event that Mercy Regional College experiences a data breach (or suspects that a data breach has occurred).

Definition

Data Breach

A data breach occurs when personal information is lost or subjected to unauthorised access, modification, use or disclosure or other misuse. Data breaches can be caused or exacerbated by a variety of factors, affect different types of personal information and give rise to a range of actual or potential harms to individuals, agencies and organisations.

Notifiable Data Breach

Where a data breach has occurred that is likely to result in serious harm to any of the individual to whom the information relates, it is considered 'eligible' and must be reported to the Office of the Australian Information Commissioner (OAIC)

Implementation

This response plan is intended to enable Mercy Regional College to contain, assess and respond to data breaches in a timely fashion, to help mitigate potential harm to affected individuals. It clarifies the roles and responsibilities of staff, and the processes to assist the school to respond to a data breach (refer to Appendix A: Flow Chart: Data Breach Response Plan).

Some data breaches may be comparatively minor, and able to be dealt with easily without reporting to the OAIC. For example:

A staff member, as a result of human error, sends an email containing personal information to the wrong recipient. Depending on the sensitivity of the contents of the email, if the email can be recalled, or if the staff member can contact the recipient and the recipient agrees to delete the email, it may be that the issue is reported to the principal but does not require any further response.

This should be documented including:

- Description of breach or suspected breach
- Action taken by the principal to address the breach or suspected breach
- The outcome of the action
- The principal's view that no further action is required

The Principal will use their discretion in determining whether a data breach or suspected data breach requires an escalation of the data breach process. In making that determination, principal will consider the following questions:

- Are multiple individuals affected by the breach or suspected breach?
- Is there (or may there be) a real risk of serious harm to the affected individual(s)?
- Does the breach or suspected breach indicate a systemic problem in school processes or procedures?
- Could there be media or stakeholder attention as a result of the breach or suspected breach?

If the answer to any of these questions is 'yes', then it may be appropriate for the principal to notify the OAIC (refer to Risk Assessment Process).

OAIC Advice Data Breach: What must be included will assist the principal in notifying the OAIC.
<https://www.oaic.gov.au/resources/agencies-and-organisations/guides/data-breach-notification-guide-august-2014.pdf>

Record Management

Documents on breaches will be saved in a central file on school administration system.

Refer to:

- Appendix A: Flow Chart: Data Breach Response Plan

Appendix A: Flow Chart: Data Breach Response Plan

